ServSelect IP Software Installation and User's Guide

Table of Contents

Features and benefits 1
System components 2
Glossary 3
Operating features 4
Target device naming *4*
Installing the software 8
Uninstalling the software 9
Opening the software 10
Setting up the software 10
Window features 13
Customizing the window display *15*
Adding an appliance 15
Accessing appliances 18
Accessing target devices 19
Customizing properties 21
Viewing and changing general properties *21*
Viewing and changing network properties *22*
Viewing and changing information properties *22*
Viewing connections properties *23*
Customizing options 23
Viewing and changing general options *24*
Managing folders 26
Assigning units 27
Deleting 28
Renaming 29
Managing the software database 29
Saving and loading a database *30*
Exporting a database *30*
Video session types 32
Using preemption 33
Preemption of a user by an administrator *34*
Preemption of a local user/administrator by an administrator *34*
Using exclusive mode 35
Using digital share mode 36
Using stealth mode 37
Using scan mode 38
Accessing scan mode *39*
Setting scan options *39*

Managing the scan sequence *40*
Using the Thumbnail Viewer *40*
Window features 41
Adjusting the view 42
Additional video adjustment *43*
Adjusting mouse options 45
Cursor type *45*
Scaling *46*
Single cursor mode *46*
Adjusting general options 46
Adjusting the Video Viewer toolbar 47
Setting the Toolbar Hide Delay time *48*
Using macros 48
Sending macros *49*
Selecting the macro group to display *49*
Using virtual media 49
Virtual Media window *50*
Virtual media session settings *51*
Opening a virtual media session *52*
Mapping virtual media drives *52*
Displaying virtual media drive details *53*
Resetting USB media devices *53*
Closing a virtual media session *54*
Managing Global settings 56
Configuring Global Network settings *56*
Configuring Global Session settings *58*
Configuring Global Virtual Media settings *60*
Configuring Global Authentication settings *62*
Configuring LDAP 63
LDAP authentication configuration parameters *63*
LDAP server parameters *64*
LDAP search parameters *65*
LDAP Query Parameters *66*
Appliance and target device query modes *68*
Setting up Active Directory for performing queries *70*
Managing local user accounts 71
Access levels *71*
Locking and unlocking user accounts *74*
Managing user sessions 75

Viewing and changing Server Access Module settings 76
Using SNMP 78
Managing SNMP traps *80*
Viewing target device connection information 82
Modifying target device names *82*
Resynchronizing the target device list *84*
Configuring cascade switch connections 84
Viewing appliance and SAM cable version information 86
Licensing appliance options 86
Upgrading firmware 86
Automatic firmware upgrades *86*
Upgrading KV2116, KV4116, or ServSelect III VM appliance firmware *87*
Upgrading SAM cable firmware *88*
Rebooting the appliance 89
Managing the appliance configuration database 90
Saving an appliance configuration database *90*
Restoring an appliance configuration database *91*
Managing the appliance user database 91
Saving an appliance user database *92*
Restoring an appliance user database *92*

Appendixes 93

Appendix A: Updating ServSelect IP Software 93
Appendix B: Virtual media 94
Appendix C: Keyboard and mouse shortcuts 96
Appendix D: Ports used by the software 98
Appendix E: Getting help and technical assistance 99
Appendix F: Notices 101

Index 103

1. Product overview

About ServSelect IP Software

With ServSelect IP Software, a cross-platform management application, you can view and control network appliances and attached target devices. The cross-platform design offers compatibility with most commonly-used operating systems and hardware platforms. Each appliance handles authentication and access control individually, placing system control at the point of need.

The software utilizes browser-like navigation with a split-screen interface, providing you with a single point of access for all appliances. Use the software to manage existing appliances, install a new target device, or open a session to a target device. Built-in groupings such as Devices, Sites, and Folders provide a way to select the units to view. Use the search and sort capabilities to find any unit.

1.1 Features and benefits

Easy to install and configure

Wizard-based installation and online help simplify initial system configuration. You can use the graphical interface to manage and update appliances, target devices, and Server Access Module (SAM) cables.

Powerful customization capabilities

You can tailor the software to fit specific system needs, using built-in groups or creating your own. You can customize unit names, field names, and icons for maximum flexibility and convenience. Use names that are meaningful to you to quickly find any target device.

Authentication and authorization

Depending on how each appliance is configured, you can authenticate and authorize users by using either the appliance database or the Lightweight Directory Assistance Protocol (LDAP). LDAP is a vendor-independent protocol standard used for accessing, querying, and updating a directory using TCP/IP. Based on the X.500 directory services model, LDAP is a global directory structure that supports strong security features including authentication, privacy, and integrity. For more information on using LDAP authentication see “Configuring Global Authentication settings” on page 72.

After users log in to an appliance, the software caches their credentials (user name and password) for the duration of the ServSelect IP Software session.

1.2 System components

The software contains the following major components.

ServSelect IP Software Explorer

The ServSelect IP Software Explorer is the primary point of control for accessing the software features and functionality. It is the main Graphic User Interface (GUI) that displays on screen when the software is opened. From the Explorer, you can easily view the appliances and target devices defined in the local database. Built-in groupings such as Appliances and Devices provide a way to list units. You can create custom groups of units

by adding and naming folders. Other groupings are also available, based on custom fields that you can assign to units.

From the ServSelect IP Software Explorer, you can select a target device from a Unit list, then click an icon to open a session to it. You can also select an appliance, then click an icon to start management and control functions.

Video Viewer

Control the keyboard, monitor, and mouse functions of individual target devices with the Video Viewer. You can use predefined macros and choose which macro group is displayed on the Video Viewer Macros menu. You can open the Video Viewer for target devices on KV2116, KV4116, or ServSelect III VM appliances.

The Video Viewer also provides access to the Virtual Media window. You can use the Virtual Media window to map drives from a target device to physical drives, such as a disk, CD, or DVD drive, on the client computer. For more information on the Virtual Media window, see “Using virtual media” on page 49.

Appliance Management Panels (AMPs)

Each AMP is implemented as a network management module that supports a target device type, such as keyboard, video, and mouse (KVM). An AMP contains a tabbed pane; each tab represents a top-level function category for the appliance. For example, the AMP tabs can be **Settings**, **Status**, and **Tools**. The number and content of tabbed panes differs for each appliance.

1.3 Glossary

The following words are used throughout this documentation:

- **ACI port connection** – a Cat5 cable connection between the ARI port of the KV2116 or KV4116 to an ACI-enabled KVM switch, allowing for integration of that KVM switch with the ServSelect IP Software
- **appliance** or **switch** (these terms are used interchangeably) - equipment that provides KVM-over-IP connectivity to attached target devices
- **cascade** or **tier** (these terms are used interchangeably) – connection between multiple KVM appliances that allows full keyboard and mouse input control and target device management from a single KVM appliance

  For example, the tiering of an analog KVM appliance under a digital KVM appliance will allow keyboard and mouse input control to all target devices attached to that analog KVM appliance via the ServSelect IP Software interface. This can either be connected through a cascade switch or an ACI port connection.
- **cascade switch** – an earlier-model analog KVM appliance that is connected to a PS2M SAM cable attached to the ARI port of a ServSelect III VM, KV2116, or KV4116 appliance, allowing for integration of an existing earlier-model switch configuration with the ServSelect IP Software
- **SAM cable** - a Server Access Module cable that, when attached to the appliance and a target device, provides additional functionality such as virtual media sessions
- **switching system** - a set of appliances and attached target devices and SAM cables
- **target device** - equipment such as a server or router that is attached to an appliance
- **unit** - includes appliances and target devices; this term is used when the procedure is referring to either or both

- **user** - a KVM connection from an analog port on the appliance
- **virtual media** - a USB media device that can be attached to the appliance and made available to any target device that is connected to the appliance

1.4 Operating features

"Keyboard and mouse shortcuts" on page 118 lists the Explorer navigation shortcuts. Other components also support full keyboard navigation in addition to mouse operations.

Target device naming

The software requires that each appliance and target device have a unique name. To minimize the need for operator intervention, the software uses the following procedure to generate a unique name for a target device whose current name conflicts with another name in the database.

During background operations (such as an automated operation that adds or modifies a name or connection), if a name conflict occurs, the conflicting name is automatically made unique. This is done by appending a tilde (~) followed by an optional set of digits. The digits are added in cases where adding the tilde alone does not make the name unique. The digits start with a value of one and are incremented until a unique name is created.

During operations, if you or another user specifies a non-unique name, a message informs the corresponding user that a unique name is required.

Target device name displays

When an appliance is added, the target device names retrieved from the appliance are stored in the software database. The operator can then rename a target device in the Explorer. The new name is stored in the database and used in various component screens. This new target device name is not communicated to the appliance.

You can change target device names on both the appliance and the database by using the Modify Device Name window in the AMP. For more information see "Modifying target device names" on page 87.

Since the software is a decentralized management system, you can change the name assigned to a target device on the appliance at any time without updating the software database. Each operator can customize a particular view of the list of target devices being managed.

Since you can associate more than one name with a single target device - one on the appliance and one in the software - the software uses the following rules to determine which name is used:

- The Explorer only shows the target devices listed in its database, with the name specified in the database. In other words, the Explorer does not talk to the appliance to obtain target device information.
- The AMP displays information retrieved from the appliance, except where noted.
- The Resync Wizard (which is used to resynchronize target device lists in the AMP) overwrites locally-defined target device names only if the appliance target device name has been changed from the default value. Non-default target device names that are read from the appliance during a resynchronization override the locally-defined names.

Sorting

In certain displays, the software component displays a list of items with columns of information about each item. If a column header contains an arrow, you can sort the list by that column in ascending or descending order.

To sort a display by a column header, click the arrow in a column header. The items in the list are sorted according to that column. An upward-pointing arrow indicates the list is sorted by that column header in ascending order. A downward-pointing arrow indicates the list is sorted by that column header in descending order.

2. Installation and startup

Getting started

Before you install the software, make sure that you have all the required items.

Supplied with ServSelect IP Software

The following items come with the ServSelect IP Software:

- Documentation CD
- ServSelect IP Software CD
- Download instructions

Supported operating systems

The following operating systems are supported by the ServSelect IP Software:

- Microsoft® Windows® 2000 Workstation Service Pack 4
- Microsoft Windows 2000 Server Service Pack 4
- Microsoft Windows XP (Home and Professional) Service Pack 2
- Microsoft Windows Server 2003 Service Pack 1
- Red Hat Enterprise Linux 3.0 WS
- Red Hat Enterprise Linux 4.0 WS
- SuSE Linux Enterprise Server 8
- SuSE Linux Enterprise Server 9
- SuSE Linux 9.2
- SuSE Linux 9.3

Hardware configuration requirements

The software is supported on the following minimum computer hardware configurations:

- 500 MHz Pentium III
- 256 MB RAM
- 10BASE-T or 100BASE-T NIC
- XGA video with graphics accelerator
- Desktop size must be a minimum of 800 x 600
- Color palette must be a minimum of 65,536 (16-bit) colors

Browser requirements

You will need one of the following browsers installed on the computer to run the ServSelect IP Software:

- Internet Explorer 5.0 or later (Windows only)
- Netscape 6.0 or later
- Mozilla™ 1.4 or later
- Firefox 1.0 or later

2.1 Installing the software

To install on Microsoft Windows operating systems, complete the following steps:

1. Insert the ServSelect IP Software CD into the CD drive. Complete one of the following steps:
   - If AutoPlay is supported and enabled, the setup program starts automatically.
   - If the computer does not support AutoPlay, set the default drive to the CD drive letter and execute the following command to start the install program (replace "drive" with the CD drive letter on the system):
     drive:\ServSelect IP Software\win32\setup.exe
2. Follow the on-screen instructions.

To install on Linux operating systems, complete the following steps:

1. Insert the ServSelect IP Software CD into the CD drive. Complete one of the following steps:
   - When using Red Hat and SUSE Linux distributions, the CD will usually be mounted automatically.

     Continue with step 2 if the CD mounts automatically.
   - If the CD does not mount automatically, you might need to issue the mount command manually. The following is an example of a typical mount command:

     mount -t iso9660 *device_file mount_point*

     where *device_file* is the system-dependent device file associated with the CD and *mount_point* is the directory that will be used to access the contents of the CD after it is mounted. Typical default values include "/mnt/cdrom" and "/media/cdrom".

     See the Linux operating system documentation for the specific mount command syntax to use.
2. Open a command window and navigate to the CD mount point. For example:
   cd /mnt/cdrom
3. Enter the following command to start the install program:
   sh ./ServSelect IP Software/linux/setup.bin
4. Follow the on-screen instructions.

During installation

You are prompted to select the destination location where the application will be installed. You can select an existing path or type a directory path. The default path for Windows 2000, NT, and XP systems is the program files directory. The default path for Linux systems is the usr/lib directory.

If you enter a path that does not exist, the installation program automatically creates it during installation.

You can also indicate if you want a ServSelect IP Software icon installed on the desktop.

2.2 Uninstalling the software

To uninstall the software on Microsoft Windows operating systems, starting at the Control Panel, complete the following steps:

1. Open the Control Panel and select **Add/Remove Programs**. A sorted list of currently installed programs opens.
2. Select the ServSelect IP Software entry.
3. Click the **Change/Remove** button. The uninstall wizard starts.
4. Click the **Uninstall** button and follow the on-screen instructions.

To uninstall the software on Microsoft Windows operating systems, using a command window, complete the following steps:

1. Open a command window and change to the ServSelect IP Software install directory used during installation. The default path for win32 systems is the program files directory.
2. Change to the UninstallerData subdirectory and enter the following command (the quotation marks are required):

   ```
   "Uninstall Black Box ServSelect IP Software.exe"
   ```

   The uninstall wizard starts. Follow the on-screen instructions.

To uninstall the software on Linux operating systems, complete the following steps:

1. Open a command window and change to the ServSelect IP Software install directory used during installation. The default path for Linux systems is the usr/lib directory.
2. Change to the UninstallerData subdirectory and enter the following command:

   ```
   sh ./Uninstall_Black Box_ServSelect_IP_Software
   ```

   The uninstall wizard starts. Follow the on-screen instructions.

2.3 Opening the software

To open the software on Microsoft Windows operating systems, complete one of the following steps:

- Select **Start > Programs > ServSelect IP Software**.
- Double-click the **ServSelect IP Software** icon.

To open the software on Linux from the application folder (the default location is /usr/lib/Black Box_ServSelect_IP_Software/), complete one of the following steps:

- Enter the command: ./ServSelect_ IP_Software
- From (/user/bin), enter the following link: ./Black Box_ServSelect_IP_Software
- If a desktop shortcut was created on installation, double-click the shortcut.

2.4 Setting up the software

This section provides an overview of setup and configuration steps. Details are provided in other chapters. For appliance-specific information, see the *Installation and User's Guide* for the appliance.

To set up the software, complete the following steps:

1. Install the software on each computer.
2. From one computer, open the software.
3. Complete one of the following steps:
   - Click the **New Appliance** button to add an appliance to the software database. The New Appliance Wizard opens.
   - Select **Tools > Discover** from the software menu to search for all KV2116, KV4116, and ServSelect III VM appliances.
4. Use the Explorer to set unit properties, options, and other customization as needed.
5. Select an appliance and click the **Manage Appliance** button to create local user accounts through the appliance AMP.
6. From the AMP **Devices** category, set the names of all target devices.
7. Repeat steps 3 through 6 for each KV2116, KV4116, and ServSelect III VM appliance you want to manage.
8. After one ServSelect IP Software environment is set up, select **File > Database > Save** to save a copy of the local database with all the settings.
9. From the software on a second computer, select **File > Database > Load** and browse the file you have saved. Select the file and then click **Load**. Repeat this step for each client computer that you want to setup.
10. To access a target device attached to an appliance, select the target device in the Explorer and click the **Connect Video** or **Browse** button to open a session (only the corresponding button for the selected target device is visible).

For information about creating user accounts on an LDAP directory service, see "Configuring LDAP" on page 73.

To set up a KV2116, KV4116, or ServSelect III VM appliance, complete the following steps:

1. Adjust mouse acceleration on each target device to **Slow** or **None**.
2. Install the appliance hardware, connect the SAM cables and connect the keyboard, monitor, and mouse to the analog port.
3. Connect a terminal to the serial configuration port on the rear panel of the appliance and set up the network configuration (network speed and address type).
4. At the local analog computer, input all target device names using the OSD interface. You can also input target device names using the ServSelect IP Software.

3. ServSelect IP Software Explorer

About the ServSelect IP Software Explorer

The ServSelect IP Software Explorer (which is called Explorer from here on) is the main GUI interface for the software. You can view, access, manage, and create custom groupings for all supported units.

When you start the software, the main Explorer window opens.

3.1 Window features

The Explorer window is divided into several areas: the View Selector buttons, the Group Selector pane, and the Unit Selector pane. The content of these areas changes, based on whether a target device or an appliance is selected or what task is to be completed. Figure 3-1 on page 14 shows the window areas; descriptions follow in Table on page 14.

Click one of the **View Selector** buttons to view the switching system organized by categories: **Appliances**, **Devices**, **Sites**, or **Folders**. The Explorer's default display is user-configurable. For more information, see "Customizing the window display" on page 14.

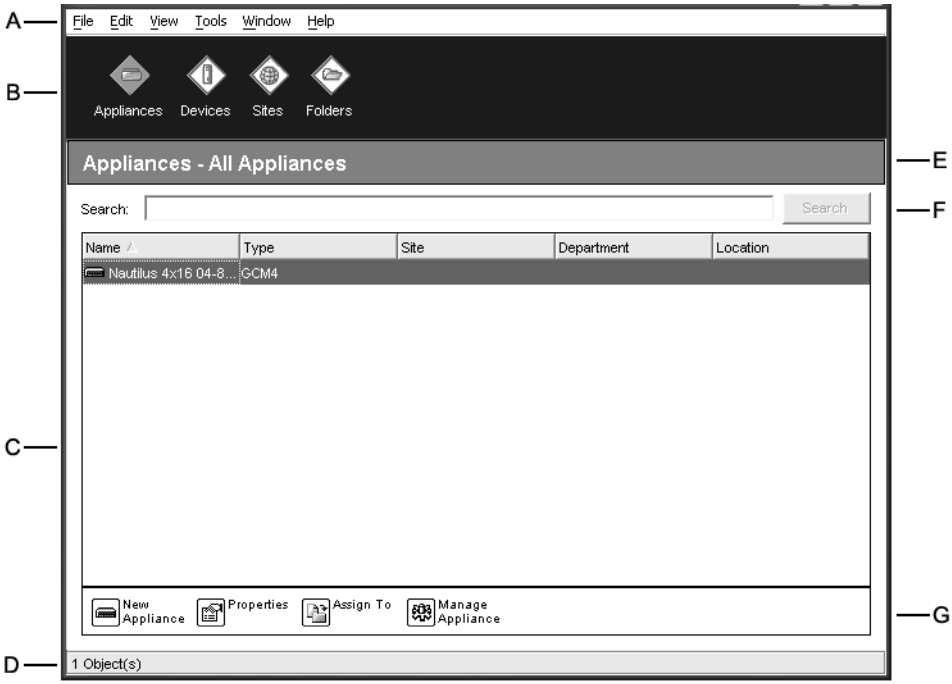

Figure 3-1. Explorer window areas

Explorer window areas

Area	Description
A	**Menu bar:** Provides access to many of the features in the software.
B	**View Selector pane:** Contains View Selector buttons for choosing the Explorer view. C button shows the switching system organized by the button category: **Appliances**, **Dev Sites**, or **Folders**. You can configure which button is visible by default.
C	**Unit list:** Displays a list of target devices, appliances, and other selectable units contain currently selected group, or the results of the search executed from the Search bar.
D	**Status bar:** Displays the number of units shown in the Unit list.
E	**Unit Selector pane:** Contains the Search bar, Unit list, and Task buttons that correspon selected view or group.
F	**Search bar:** Gives you the ability to search the database for the text entered in the **Sea**
G	**Task buttons:** Represent tasks that can be executed. Some buttons are dynamic, base unit selected in the Unit list, while other buttons are fixed and always present.

Customizing the window display

You can resize the Explorer window at any time. Each time you start the application, the Explorer window opens to its default size and location.

A split-pane divider that runs from top to bottom separates the Group Selector pane and the Unit Selector pane. You can move the divider left and right to change the viewing area of these two panes. Each time the Explorer is opened, the divider returns to its default location. See “Keyboard and mouse shortcuts” on page 118 for divider pane and tree view control shortcuts.

You can specify which view (Appliances, Devices, Sites, or Folders) is visible on startup or you can let the Explorer determine it. For more information, see “Selected view on startup” on page 26.

You can change the order and sorting of the Unit list by clicking the sort bar above the column. An upward-pointing arrow in a column header indicates that the list is sorted by that field name in ascending order. A downward-pointing arrow indicates the list is sorted by that field name in descending order.

3.2 Adding an appliance

Before you can access the appliance through the software, you must add it to the software database. After an appliance is added, it is visible in the Unit list. You can either manually add or discover an appliance.

To manually add an appliance with an assigned IP address, complete the following steps:

1. Complete one of the following steps:

- Select **File > New > Appliance** from the Explorer menu.
- Click the **New Appliance** button.

The New Appliance Wizard opens. Click **Next**.

2. Select the type of appliance you are adding. Click **Next**.
3. Click **Yes** to indicate that the appliance has an assigned IP address, then click **Next**.
4. Type the IP address and click **Next**.
5. The software searches for the appliance.

   The software searches for the indicated unit as well as all the powered SAM cables and target device names you associated with it in the OSD, if any. To search for unpowered SAM cables, you can access the resync feature in the **Devices** category of the AMP and select the **Include Offline Server Access Modules** check box.

   The Enter Cascade Switch Information window opens if the software detects an attached cascade switch. This window contains a list of all ports and SAM cable eIDs (Electronic Identification Numbers) retrieved from the appliance and the tiered switch types to which they are connected, if any. When this window first opens, all appliances are set to **None**. Detected appliances have an icon next to the pull-down menu.

   a. The **Existing Cascaded Switches** field contains all the current cascade switch types defined in the database. Click **Add**, **Delete**, or **Modify** to alter the list.

   b. Associate the applicable cascade switch types from the pull-down menus for each SAM cable that has a cascade switch attached.

6. When you reach the final page of the Wizard, click **Finish** to exit the Wizard and return to the main window. The appliance is now included in the Unit list.

To discover an appliance by IP address, complete the following steps:

1. Select **Tools > Discover** from the Explorer menu. The Discover Wizard opens. Click **Next**.
2. The Address Range page opens. Type the range of IP addresses to search on the network in the To and From boxes. Use IP address dot notation. Click **Next**.
3. Complete one of the following steps:
   - The Searching Network progress window opens. Progress text indicates how many addresses have been probed from the total number specified by the range, and the number of appliances found (for example, 21 of 100 addresses probed: 3 appliances found). If one or more new appliances are discovered, the Wizard shows the Select Appliances to Add page. From this page, you can select the appliances to add to the local database.
   - If no new appliances were found (or if you clicked **Stop**), the Wizard shows the No New Appliances Found page. You can try entering a different range to search or add the appliances manually.
   - **SCPS** - When the specifi ed SCPS is found, it will be polled for server information. However, you are given the opportunity to indicate if ports confi gured with default names should be excluded. If these are excluded, those servers are not added to the database.
   - **ServSelect IP** - ServSelect IP Software will search for the indicated unit as well as all the powered SAM and server names you associated with it in the OSD, if any. To search for unpowered SAM adaptors, you may access the resync feature

in the Servers category of the ServSelect IP AMP and enable the *Include Offl ine SAM adaptors* checkbox. Click *Next.* The Confi gure Cascade Switches dialog box appears if ServSelect IP Software detects an attached legacy or analog switch. This box contains a list of all SAM adaptor EIDs retrieved from the appliance and the cascade switches to which they are connected, if any. When this dialog box first displays, all switches will be set to *None*. Detected switches will have an icon next to the pulldown menu.

4. Select one or more appliances to add and click the **Add (>)** icon to move the selection or selections to the Appliances to Add list. When the Appliances to Add list contains all the appliances you want to add, click **Next**.
5. The Adding Appliances progress bar window opens. Once all of the appliances have been added to the local database, the Discover Wizard Completed page opens. Click **Finish** to exit the Wizard and return to the main window. The new appliance is now visible in the Unit list.

   If one or more appliances cannot be added to the local database for any reason, the Discover Wizard Not All Appliances Added page opens. This page lists all of the appliances that you selected and the status for each. The status indicates if an appliance was added to the local database and if not, why the process failed. Click **Done** when you are finished reviewing the list.

If an appliance already exists in the database with the same IP address as a discovered unit, then the discovered unit is ignored and is not listed on the next Wizard page.

The Discover Wizard does not automatically find target devices attached to the appliance. After running the Discover Wizard, access the applicable AMP and click the **Resync** button on the **Devices** category to find target devices attached to the appliance.

To manually install a new appliance with no assigned IP address, complete the following steps:

1. Complete one of the following steps:
   - Select **File > New > Appliance** from the Explorer menu
   - Click the **New Appliance** button.

   The New Appliance Wizard opens. Click **Next**.
2. Click **No** to indicate that the appliance does not have an assigned IP address, then click **Next**.
3. The Network Address window opens. Type the IP address, subnet mask, and gateway you want to assign to the appliance and then click **Next**.
4. The software searches for any KV2116, KV4116, or ServSelect III VM appliances that do not have assigned IP addresses. Select the unit to add from the list of new appliances that were found and then click **Next**.
5. The Configuring Appliance window indicates whether the IP information was configured. If the configuration is complete, the software searches for the new appliance. Click **Next**.

   The software also searches for all SAM cables and target device names associated with the appliance.

   The Enter Cascade Switch Information window opens if the software detects an attached cascade switch. This window contains a list of all ports and SAM cable eIDs

retrieved from the appliance and the cascade switch types to which they are connected, if any.

a. The Existing Cascaded Switches field contains all the current cascade switch types defined in the database. Click **Add**, **Delete**, or **Modify** to alter the list.

b. Associate the applicable cascade switch type from the pull-down menus for each SAM cable that has a cascade switch attached.

6. When complete, click **Finish** to exit the Wizard and return to the main window. The appliance is now included in the Unit list.

3.3 Accessing appliances

Clicking the **Appliances** button opens a list of the appliances currently defined in the local database. The Group Selector pane is visible if two or more appliance types are defined. Click **All Appliances** or click on a folder to view all appliances of a particular type.

A user name and password prompt opens if this is the first unit access attempt during the ServSelect IP Software session. After a unit is accessed, subsequent access attempts for any unit that uses the same user name and password credentials during this ServSelect IP Software session do not require a user name and password. The software provides credential caching that captures credentials upon first use and automates the authentication of subsequent unit connections.

To clear login credentials, open the Explorer and go to **Tools** > **Clear Login Credentials**.

Accessing the appliance opens the AMP for that appliance. For more information, see the "Appliance Management Panel" chapter beginning on page 69.

To log in to an appliance, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on an appliance in the Unit list.
   - Select an appliance, and then click the **Manage Appliance** button.
   - Right-click on an appliance. A pop-up menu opens. Select **Manage Appliance** from the pop-up menu.
   - Select an appliance in the Unit list and press Enter.
3. If a user name and password prompt opens, type the user name and password. [If this is the first appliance access since initialization or reinitialization, the default user name is Admin (case sensitive) with no password.]
4. Complete one of the following steps:
   - Click **OK** to access the appliance. This opens the AMP for the appliance. For more information about the AMP, see "Appliance Management Panel" chapter beginning on page 69.
   - Click **Cancel** to exit without logging in.

3.4 Accessing target devices

Clicking the **Devices** button opens a list of target devices such as servers, routers, and other managed equipment that is defined in the local database. The Group Selector pane is

visible if two or more device types are defined. Click **All Devices** or click on a folder to view all target devices of a particular type.

A user name and password prompt opens if this is the first unit access attempt during the ServSelect IP Software session. After a unit is accessed, subsequent access attempts for any unit that uses the same user name and password credentials during this ServSelect IP Software session do not require a user name and password. The software provides credential caching that captures credentials upon first use and automates the authentication of subsequent unit connections.

To clear login credentials, in the Explorer go to **Tools** > **Clear Login Credentials**.

When you select a device and click the **Connect Video** button, the Video Viewer launches. The Video Viewer allows you full keyboard, video and mouse control over a device. If a URL has been defined for a given device, then the **Browse** button will also be available. The **Browse** button will launch the configured Web browser, if any, or default browser to the defined URL for that device.

For more information, see "Customizing properties" on page 20 and "Customizing options" on page 25.

If a server is connected to an SCPS that has SSH enabled, the configured Telnet access (Serial Console Viewer or third party Telnet client) will be launched on top of an SSH tunnel when required or requested.

You can also scan through a customized list of devices using the **Thumbnail Viewer**. This view contains a series of thumbnail frames, each containing a small, scaled, non-interactive version of a device screen image. For more information, see "Using scan mode" on page 39.

To access a target device, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on a target device in the Unit list.
   - Select a target device, and then click the connection button: **Connect Video** if connected to a KV2116, KV4116, or ServSelect III VM appliance or **Browse** if a URL is configured. Only the applicable button or buttons for the selected target device are visible.
   - Right-click on the target device. Select the connection entry from the pop-up menu: **Connect Video** for a KV2116, KV4116, or ServSelect III VM appliance or **Browse** if a URL is configured. Only the applicable entry for the selected target device is visible.
   - Select a target device in the Unit list and press Enter.
3. If a browser is used for access, no user name and password prompt opens.

   If the Video Viewer is used for access, a user name and password prompt opens if this is the first access attempt during the ServSelect IP Software session.

   After a unit is accessed, subsequent access attempts for any unit that uses the same user name and password credentials during this ServSelect IP Software session do not require a user name and password.

The configured access method for that target device opens in a new window.

To search for a target device in the local database, complete the following steps:

1. Click the **Devices** button and insert the cursor in the **Search** field.
2. Type the search information. This could be a target device name or a property such as type or location.
3. Click the **Search** button. The results are included in the Unit list.
4. Complete one of the following steps:
   - Review the results of the search.
   - Click the **Clear Results** button to open the entire list again.

To auto search by typing in the Unit list, complete the following steps:

1. Click the **Devices** button, then click on any item in the Unit list.
2. Begin typing the first few characters of a target device name. The highlight moves to the first target device name beginning with those characters. To reset the search so you can find another target device, pause for a few seconds and then type the first few characters of the next target device.

If the target device you are attempting to access is currently being viewed by another user, you can preempt the user so you can have access to that target device, or request a shared session with that user (KVM sharing is only available on KV4116 and KV2116 appliances). For more information, see “Using preemption” on page 34 and “Using digital share mode” on page 37.

To confi gure Serial Console Viewer access to a server via the SCPS:

NOTE: Serial Console Viewer access is enabled by default. The following procedure is provided in the event you confi gure another access method and later wish to return to using this method.

1. To configure the Serial Console Viewer as the global default access method:
   a. Select *Tools - Options* from the ServSelect IP Software Explorer menu.
   b. Click the *Telnet* tab.
   c. Enable the *Launch built-in application* checkbox.
   d. Click *OK* to save the settings.
2. If the global default is set for a method other than the built-in application, and you wish to override it for this server:
   a. Select a unit from the Unit list.
   b. Select *View - Properties* from the ServSelect IP Software Explorer menu.

-or-

Click the *Properties* task button.

-or-

Right-click on the unit. Select *Properties* from the pop-up menu. The

Properties dialog box appears.

   c. Enable the *Launch built-in application* checkbox.
3. Click *OK* to save the settings.

To confi gure third party Telnet access to a server via the SCPS:

1. To confi gure a third party Telnet application as the global default access method:

a. Select *Tools - Options* from the ServSelect IP Software Explorer menu.
b. Click the *Telnet* tab.
c. Enable the *Launch user-specifi ed application* checkbox. Enter the directory path, name and any command line arguments. For commands that do not provide a GUI, enable the *Launch in command window* checkbox.
d. Click *OK* to save the changes.

2. If the global default is set for a method other than that user-specified Telnet application, and you wish to override it for this server:
   a. Select a unit from the Unit list.
   b. Select *View - Properties* from the ServSelect IP Software Explorer menu.

-or-

Click the *Properties* task button.

-or-

Right-click on the unit. Select *Properties* from the pop-up menu. The Properties dialog box appears.

   c. Enable the *Launch user-specifi ed application* checkbox and enter the directory path, name and any command line arguments. For commands that do not provide a GUI, enable the *Launch in command window* checkbox.

To confi gure Telnet access directly to a server:

NOTE: This procedure applies to Serial Console Viewer or third party Telnet access directly to a server.

1. Select *View - Properties* from the ServSelect IP Software Explorer menu.

-or-

Click the *Properties* task button.

-or-

Right-click on the unit. Select *Properties* from the pop-up menu. The Properties dialog box appears.

2. Click the *Telnet* tab.
3. Specify the server's IP address and enable the *Use Default* checkbox. The port number defaults to 23; you may specify another value.
4. Click *OK* to save the changes.

3.5 Customizing properties

The Properties window in the Explorer contains the following tabs: **General**, **Network**, **Information**, and, if the selected unit is a device, **Connections**. Use these tabs to view and change properties for the selected unit.

You may alter certain properties of individual appliances and servers using ServSelect IP Software Explorer. The Properties dialog box in the ServSelect IP Software Explorer contains five tabs: General, Network, Information, Connections and Telnet.

General properties

General properties describe the unit and its location. You may specify a unit's name, Type (server only), icon, Site, Department and Location. (You may also customize the Site, Department and Location field labels; see *Changing Options* in this chapter.) Network

properties For an appliance, network properties include the appliance's address and, for generic appliances, the URL to be used when establishing a browser connection. When this field contains a value, the Browse button appears in the ServSelect IP Software Explorer task bar.

For a server, network properties specify the URL to use when establishing a browser connection to the server. When this field contains a value, the Browse button appears in the ServSelect IP Software Explorer task bar.

Information properties

Information properties include descriptive, contact and comment information; these fields may contain any information you require.

To change information properties:

1. Select an appliance or server in the Unit list.
2. Select *View - Properties* from the ServSelect IP Software Explorer menu.
   - or -
   Click the *Properties* task button.
   - or -
   Right-click on the unit. Select *Properties* from the pop-up menu. The Properties dialog box appears.
3. Click the *Information* tab. You may enter any information in the following fields.
   a. In the Description field, enter 0-128 characters.
   b. In the Contact field, enter 0-128 characters.
   c. In the Contact Phone Number field, enter 0-64 characters.
   d. In the Comments field, enter 0-256 characters.
4. Click another tab to change additional properties.
   - or -
   If finished, click *OK* to save the new settings.
   - or -
   Click *Cancel* to exit without saving the new settings.

Connections properties

Connections properties appear only for servers and are read-only. The display indicates the physical connection path that will be used to access this server and the connection type, such as serial or video.

Telnet properties

Telnet properties include the IP address (for servers only) and the port number to connect to when establishing a Telnet session to the unit. You may designate the built-in Serial Console Viewer as the Telnet client or you may specify another Telnet application. When you specify the built-in application, you may choose to open the window before login to troubleshoot login scripts.

When you indicate a user-specified Telnet application, you may include its command line arguments. A selection of macros is available for placement in the command line; this may be useful for automatic replacement of variables such as IP address, port number, username and password. For Telnet commands that do not provide their own GUI, such as those for standard Windows, Linux and Unix, you may have the Telnet application launched from within an OS command window.

Viewing and changing general properties

In general properties, you can specify a unit Name, Type (target device only), Icon, Site, Department, and Location. (To customize the Site, Department, and Location field labels, see “Custom field names” on page 25.)

To view or change general properties, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
   - Select **View > Properties** from the Explorer menu.
   - Click the **Properties** button.
   - Right-click on the unit. Select **Properties** from the pop-up menu.

   The General Properties window opens.

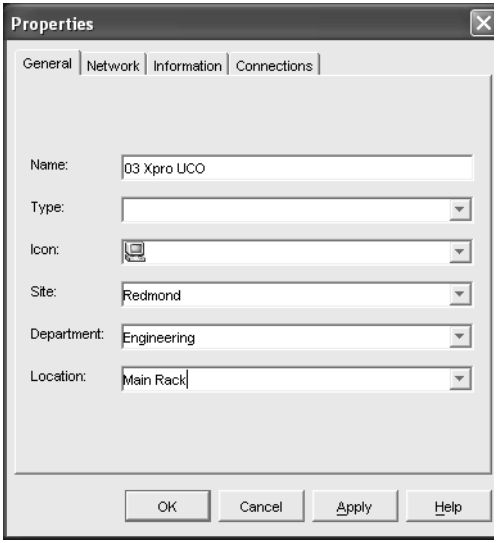

Figure 3-2. Device General Properties window

3. In the **Name** field, type a 1 to 32 character unique name. (This name is local to the software database; the appliance database might contain a different name for this unit.)
4. The **Type** field is read-only for appliances. For a target device, select a type from the pull-down menu or enter a 1 to 32 character type in the text field.
5. In the **Icon** field, select an icon from the pull-down menu.
6. In the **Site**, **Department**, and **Location** fields, select an entry from the pull-down menu or enter a 1 to 32 character Site, Department, or Location in the corresponding text field.
7. Complete one of the following steps:
   - Click another tab to change additional properties.
   - If finished, click **OK** to save the new settings.

- Click **Cancel** to exit without saving the new settings.

Viewing and changing network properties

For an appliance, network properties include the address of the appliance.

For a target device, network properties specify the URL to use when establishing a browser connection to the target device. When this field contains a value, the **Browse** button is visible in the Explorer task bar.

To view or change network properties, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
   - Select **View > Properties** from the Explorer menu.
   - Click the **Properties** button.
   - Right-click on the unit. Select **Properties** from the pop-up menu.

   The Properties window opens.
3. Click the **Network** tab.
4. In the Address field (appliances only), enter the appliance address in IP dot notation or 1 to 128 character host name. The address cannot be blank, a loopback address, or all zeros. You cannot enter duplicate addresses.
5. In the **Browser URL** field (devices only), enter a 1 to 256 character URL for establishing a browser connection.
6. Complete one of the following steps:
   - Click another tab to change additional properties.
   - If finished, click **OK** to save the new settings.
   - Click **Cancel** to exit without saving the new settings.

Viewing and changing information properties

Information properties include description, contact phone number, and comment information; you can use these fields to store any information you require.

To view or change information properties, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
   - Select **View > Properties** from the Explorer menu.
   - Click the **Properties** button.
   - Right-click on the unit. Select **Properties** from the pop-up menu.

   The Properties window opens.
3. Click the **Information** tab. You can enter any information in the following fields.
   a. In the **Description** field, enter 0 to 128 characters.
   b. In the **Contact** field, enter 0 to 128 characters.
   c. In the **Contact Phone Number** field, enter 0 to 64 characters.
   d. In the **Comment** field, enter 0 to 256 characters.
4. Complete one of the following steps:
   - Click another tab to change additional properties.
   - If finished, click **OK** to save the new settings.

- Click **Cancel** to exit without saving the new settings.

To change Telenet properties:

1. Select an appliance or server in the Unit list.
2. Select *View - Properties* from the ServSelect IP Software Explorer menu.

-or-

Click the *Properties* task button.

-or-

Right-click on the unit. Select *Properties* from the pop-up menu. The Properties dialog box appears.

3. Click the *Telnet* tab.
4. For servers only, in the IP Address field, enter an IP address in dot notation or a 1-128 character domain name. Spaces are not allowed. Duplicate addresses are allowed.
5. In the Port field, enter a port number in the range 23-65535. If blank, port 23 is used.
6. Enable/disable the *Use Default* checkbox. When enabled, the default global setting specifi ed in Options will be used, and all other portions of the Application to Launch area are disabled.
7. Enable/disable the *Launch built-in application* checkbox. When enabled, the built-in Serial Console Viewer application will be used to connect to this unit. If you enable the *Launch built-in application* checkbox, you may also enable/ disable the *Open Window before login* checkbox. When this checkbox is enabled, the Serial Console Viewer Telnet window will open before any login attempt is made to the server. This feature is useful when debugging a login script, and is usually disabled otherwise.
8. Enable/disable the *Launch user-specifi ed* application checkbox. When enabled, the Telnet application specifi ed in the field below the checkbox will be used.
    a. Enter the directory path and name or click the *Browse* button to locate the path and name.
    b. Enter command line arguments in the box below the path and name.
    c. To insert a predefi ned macro at the cursor location in the command line,click the *Insert Macro* list box and select a macro from the pulldown menu. ServSelect IP Software will automatically replace these variables when the application runs.
    d. Enable/disable the *Launch in command window* checkbox. When enabled, the user-specifi ed Telnet application will be launched from within an OS command window.
9. Click another tab to change additional properties.

-or-

If finished, click *OK* to save the new settings.

-or-

Click *Cancel* to exit without saving the new settings.

Viewing connections properties

Connections properties are available only for target devices and are read-only. The display indicates the physical connection path that is used to access this target device and the connection type, such as video.

To view connections properties, complete the following steps:

1. Select a target device in the Unit list.
2. Complete one of the following steps:
   - Select **View > Properties** from the Explorer menu.
   - Click the **Properties** button.
   - Right-click on the unit. Select **Properties** from the pop-up menu.

   The Properties window opens.
3. Click the **Connections** tab.

3.6 Customizing options

Set general options for the Explorer in the Options window. General options include custom field names, selected view on startup, browser application, and DirectDraw support.

Viewing and changing general options

You can customize options for the Explorer, including custom name fields, default view, and default browser.

Custom field names

In the Custom field labels area, you can change the Site, Department, and Location headings that are visible in the Group and Unit Selector panes. You can group units in ways that are meaningful to you. The **Department** field is a subset of Site.

To change custom field names, complete the following steps:

1. Select **Tools > Options** from the Explorer menu. The General Options window opens.

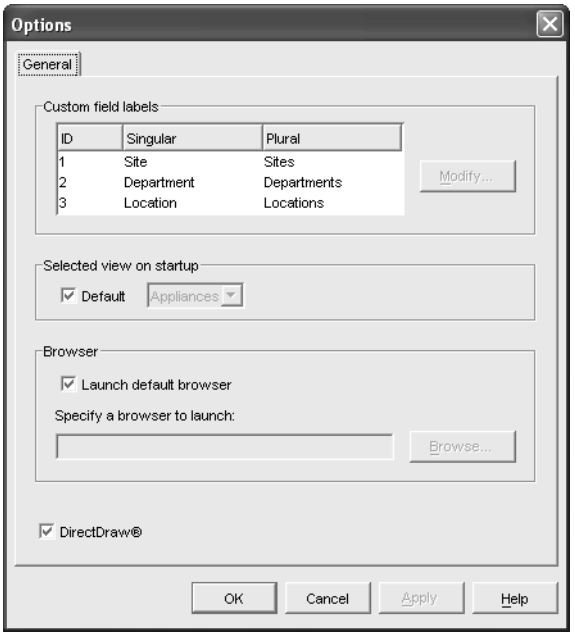

Figure 3-3. General Options window

2. In the Custom field labels area, select a field label to modify and click the **Modify** button. The Modify Custom Field Label window opens. Remember that the **Department** field is a subset of the **Site** field, even if it is renamed. Type the 1 to 32 character singular and plural versions of the new field label. You can use embedded spaces but not leading or trailing spaces. You cannot use blank field labels.
3. Complete one of the following steps:
   - If finished, click **OK** to save the new settings.
   - Click **Cancel** to exit without saving the new settings.

Selected view on startup

The "Selected view on startup option" specifies the view that is visible when the software opens, either Appliances, Devices, Sites, or Folders. You can select a view or let the Explorer determine the view. When you let the Explorer determine the view, the Devices view is visible if you have one or more target devices defined. If you do not, the Appliances view is visible.

To view or change the selected view on startup, complete the following steps:

1. Select **Tools > Options** from the Explorer menu. The General Options window opens.

2. Complete one of the following steps:
   - If you want the Explorer to determine the best view on startup, select the **Default** check box.
   - If you want to specify which view opens on startup, clear the **Default** check box and select **Appliances**, **Devices**, **Sites**, or **Folders** from the pull-down menu.
3. Complete one of the following steps:
   - If finished, click **OK** to save the new settings.
   - Click **Cancel** to exit without saving the new settings.

Default browser

The Browser option specifies the browser application that opens when you click the **Browse** button for a target device that has URL defined, or when the ServSelect IP Software online help is opened. You can either enable the default browser application of the current computer or select among other available browsers.

To view or change the default browser, complete the following steps:

1. Select **Tools > Options** from the Explorer menu. The General Options window opens.
2. Complete one of the following steps:
   - In the **Browser** field, select the **Launch Default Browser** check box to specify the default browser.
   - Clear the **Launch Default Browser** check box. Click the **Browse** button and select a browser executable on the computer. You can also enter the full path name of the browser executable.
3. Complete one of the following steps:
   - If finished, click **OK** to save the new settings.
   - Click **Cancel** to exit without saving the new settings.

DirectDraw support (Windows only)

The DirectDraw option affects operation of the Video Viewer when running on Windows operating systems. The software supports DirectDraw, a standard that you can use to directly manipulate video display memory, hardware blitting, hardware overlays, and page flipping without the intervention of the Graphical Device Interface (GDI). This can result in smoother animation and improvement in the performance of display-intensive software.

However, if the machine has a software cursor or pointer shadow enabled, or if the video driver does not support DirectDraw, you can experience a flicker in the mouse cursor when over the title bar of the Video Viewer. You can either disable the software cursor or pointer shadow, load a new target device driver for the video card, or disable DirectDraw.

To view or change DirectDraw support, complete the following steps:

1. Select **Tools > Options** from the Explorer menu. The General Options window opens.
2. In the DirectDraw field, select or clear the **DirectDraw** check box.
3. Complete one of the following steps:
   - If finished, click **OK** to save the new settings.
   - Click **Cancel** to exit without saving the new settings.

Telnet options

Telnet options are used when an individual server's Properties dialog box (Telnet tab) has the Use Default checkbox enabled. You may designate the built-in Serial Console Viewer as the Telnet client or you may specify another Telnet application. When you specify the built-in application, you may choose to open the window before login to troubleshoot login scripts.

When you indicate a user-specified Telnet application, you may include its command line arguments. A selection of macros is available for placement in the command line; this may be useful for automatic replacement of variables such as IP address, port number, username and password. For Telnet commands that do not provide their own GUI, such as those for standard Windows, Linux and Unix, you may have the Telnet application launch from within an OS command window.

To change Telnet options:

1. Select *Tools - Options* from the ServSelect IP Software Explorer menu. The Options dialog box appears.
2. Click the *Telnet* tab.
3. Enable/disable the *Launch built-in application* checkbox. When enabled, the built-in Serial Console Viewer application will be used to connect to a unit, if it supports Telnet connections and if the unit's properties do not override it. If you enable the *Launch built-in application* checkbox, you may also enable/ disable the *Open Window before login* checkbox. When enabled, the Serial Console Viewer Telnet window will open before any login attempt is made to the server. This feature is useful when debugging a login script, and is usually disabled otherwise.
4. Enable/disable the *Launch user-specifi ed* application checkbox. When enabled, the Telnet application specifi ed in the box below the checkbox will be used, if it supports Telnet connections and if the unit's properties do not override it.
    a. Enter the directory path and name or click the *Browse* button to locate the path and name.
    b. Enter command line arguments in the box below the path and name.
    c. To insert a predefi ned macro at the cursor location in the command line, click the *Insert Macro* list box and select a macro from the pulldown menu. ServSelect IP Software will automatically replace these variables when the application runs.
    d. Enable/disable the *Launch in command window* checkbox. When enabled, the user-specifi ed Telnet application will be launched from within an OS command window.
5. Click another tab to change additional options.

-or-

If finished, click *OK* to save the new settings.

-or-

Click *Cancel* to exit without saving the new settings.

3.7 Managing folders

Use folders to create a customized organizational system for groups of units. For example, you might create a folder for critical target devices or for remote target devices. Folders are listed under the **Folders** button in the Explorer. You can name and structure folders in any way you choose.

To create a folder, complete the following steps:

1. Select the **Folders** button.
2. Complete one of the following steps:
   - Click on the top-level **Folders** node and select **File > New > Folder**.
   - To create a nested folder, click on an existing folder and select **File > New > Folder** in the Explorer menu. The New Folder window opens.
3. Type a 1 to 32 character name. Folder names are not case sensitive. You can use embedded spaces but not leading or trailing spaces. You cannot use duplicate folder names at the same level, but you can use duplicate folder names on different levels.
4. Click **OK**. The new folder is listed in the Group Selector pane.

To assign a unit to a folder, see “Assigning units” on page 29. To rename or delete a folder, see “Renaming” on page 31 and “Deleting” on page 30.

3.8 Assigning units

After you have created a new Site, Location, or Folder, you can assign a unit to that organization. The **Assign** menu item is only enabled when a single unit is selected in the Unit list (the custom assignment targets are defined in the General Properties window).

There are three ways to assign a unit to a Site, Location, or Folder: editing the unit Properties window, using the Assign function, or dragging and dropping.

To assign a unit to a Site, Location, or Folder using the Properties window, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
   - Select **View > Properties** from the Explorer menu.
   - Click the **Properties** button. The Properties window opens.
3. Click the **General** tab. Select the Site, Department, or Location to which you want to assign the unit.
4. Complete one of the following steps:
   - Click **OK** to save the assignment.
   - Click **Cancel** to exit without saving the assignment.

To assign a unit to a Site, Location, or Folder using the Assign function, complete the following steps:

1. Select a unit in the Unit list.
2. Complete one of the following steps:
   - Select **Edit > Assign** from the Explorer menu.
   - Click the **Assign To** button.
   - Right-click on a unit and select **Assign To** from the pop-up menu.

The Assign To window opens.

3. In the Category pull-down menu, select **Site**, **Location**, or **Folder**.
4. In the Target list, select the assignment you want to designate. The target list is empty if no Site, Location, or Folder has been defined in the local database.
5. Complete one of the following steps:
   - Click **OK** to save the assignment.
   - Click **Cancel** to exit without saving the assignment.

To assign a unit to a Site, Location, or Folder using drag and drop, complete the following steps:

1. To use drag and drop, click and hold on a unit in the Unit list.
2. Drag the item on top of a folder icon (node) in the tree view of the Group Selector pane. Release the mouse button.
3. The item is now visible in the Unit list when you click that node.

A unit cannot be moved to All Departments, All Units, or the root Sites node. Units can only be moved one at a time.

3.9 Deleting

The delete function works according to what is currently selected in the Group and Unit Selector panes. When you select and delete a unit in the Unit list, it is removed from the local database. When you select and delete an item in the tree view of the Group Selector pane, you can delete Server Types, Sites, Departments, or Folders; however, none of the actions result in units being deleted from the local database.

To delete a unit, complete the following steps:

1. Select the unit or units to delete from the Unit list.
2. Complete one of the following steps:
   - Select **Edit > Delete** from the Explorer menu.
   - Right-click on a unit and select **Delete** from the pop-up menu.
   - Press the Delete key on the keyboard.
3. A window prompts you to confirm the number of units you want to delete. If you are deleting an appliance, the window includes a **Delete Associated Devices** check box. Select or clear the check box as needed. If you do not delete the associated target devices, they are still visible in the target devices list but you cannot connect to them unless they have a URL assigned, in which case you can connect to the target device using a browser.
4. Complete one of the following steps:
   - Click **Yes** to confirm the deletion. You might receive additional message prompts, depending on the configuration. Respond as needed. The units are deleted.
   - Click **No** to cancel the deletion.

To delete a target device Type, Site, Department, or Folder, complete the following steps:

1. Select the target device Type, Site, Department, or Folder to delete from the Group Selector pane.

2. Complete one of the following steps:
   - Select **Edit > Delete** from the Explorer menu.
   - Press the Delete key on the keyboard.
3. You are prompted to confirm the number of units that are affected by this deletion. Complete one of the following steps:
   - Click **Yes** to confirm the deletion. You might receive additional message prompts, depending on the configuration. Respond as needed. The element is deleted.
   - Click **No** to cancel the deletion.

3.10 Renaming

The rename function works according to what is currently selected. You might select and rename an appliance or a target device from the Unit list. You can select and rename unit Types, Sites, Departments, and Folder names in the tree view of the Group Selector pane.

To rename a unit Type, Site, Department, or Folder, complete the following steps:

1. Complete one of the following steps:
   - Select a unit from the Unit list.
   - In the Group Selector pane, select the unit Type, Site, Department, or Folder to rename.
2. Complete one of the following steps:
   - Select **Edit > Rename** from the Explorer menu.
   - Right-click on the unit Type, Site, Department, or Folder in the Unit list and select **Rename** from the pop-up menu. The Rename window opens.
3. Type a 1 to 32 character name. You can use embedded spaces but not leading or trailing spaces. (This name is local to the software database; the appliance database might contain a different name for this unit.)
4. Complete one of the following steps:
   - Click **OK** to save the new name.
   - Click **Cancel** to exit without saving changes.

For a unit Type, Site, Department, or Folder, you cannot use duplicate names, including the same name with different cases, with two exceptions: department names can be duplicated on different sites and folder names can be duplicated on different levels.

3.11 Managing the software database

Each computer running the software contains a local database that records the information that you enter about the units. If you have multiple computers, you can configure one computer and then save a copy of this database and load it into the other computers to avoid unnecessarily reconfiguring each computer. You can also export the database for use in another application.

Saving and loading a database

You can save a copy of the local database and then load it back to the same computer where it was created, or onto another computer running the software. The saved database is compressed into a single Zip file.

While the database is being saved or loaded, you cannot use or modify the database. You must close all other windows, including target device session windows and AMP windows. If other windows are open, a message prompts you to either continue and close all open windows or quit and cancel the database save process.

To save a database, complete the following steps:

1. Select **File > Database > Save** from the Explorer menu. The Database Save window opens.
2. Enter a file name and select a location to save the file.
3. Click **Save**. A progress bar is visible during the save. When finished, a message indicates that the save is complete and you are returned to the main window.

To load a database, complete the following steps:

1. Select **File > Database > Load** from the Explorer menu. The Database Load window opens.
2. Browse to select a database to load.
3. Click **Load**. A progress bar is visible during the load. When finished, a message indicates that the load is complete, and you are returned to the main window.

Exporting a database

You can export fields from the local database to a Comma Separated Value (CSV) file or Tab Separated Value (TSV) file. The following database fields are exported:

Appliance flagTypeName
AddressCustom Field 1Custom Field 2
Custom Field 3DescriptionContact Name
Contact Phone CommentsBrowser URL

The first line of the exported file contains the column names for the field data. Each additional line contains the field data for a unit. The file contains a line for each unit defined in the local database.

To export a database, complete the following steps:

1. Select **File > Database > Export** from the Explorer menu. The Database Export window opens.
2. Type a file name and browse to the location to save the exported file.
3. Click **Export**. A progress bar is visible during the export. When finished, a message indicates that the export is complete, and you are returned to the main window.

4. Video Viewer

About the Video Viewer

When you connect to a target device using the Video Viewer, the desktop of the device is visible in a separate Video Viewer window. You can see both the local cursor and the target device cursor.

From this window, you can access all the normal functions of this target device as if you were sitting in front of it. You can also perform viewer-specific tasks such as sending macro commands to the target device.

You can open the Video Viewer for target devices on KV2116, KV4116, or ServSelect III VM appliances.

If the target device you are attempting to access is currently being viewed by another user, you have several options depending on your access rights. If you are an administrator, you can share the session, preempt the session, or observe the session in stealth mode. For more information about access rights and session types, see “Video session types” on page 33 and “Managing local user accounts” on page 79.

To access the Video Viewer, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on the target device in the Unit list.
   - Select the target device, then click the **Connect Video** button.
   - Right-click on the target device. Select **Connect Video** from the pop-up menu.
   - Select the target device and press Enter.

If the target device is not being viewed by another user, the Video Viewer opens in a new window. If the target device is being accessed by another user, you might have the option to preempt the session, share the session, or observe the session in stealth mode, depending on your access rights.

If this is the first unit access of the ServSelect IP Software session, a user name and password is required.

Important: A user name and password is not required for any subsequent access attempts during the same ServSelect IP Software session unless you clear the current cached credentials.

To close a Video Viewer session, complete one of the following steps:

- Select **File > Exit** from the Video Viewer menu.
- Click **X** to close the Video Viewer session.

4.1 Video session types

When using the Video Viewer with KV2116 and KV4116 appliances, you can choose which type of session you want to operate. In addition to operating a normal KVM session, administrators and users with certain access rights can also operate a session in an exclusive mode, share the session with one or more users, observe a session in stealth mode, or scan multiple target devices. The current type of session is indicated by an icon

on the right side of the Video Viewer toolbar. Video session types are outlined in the table below.

Video session types

Session types	Icons	Description
Active (normal)		You are conducting a normal KVM session that is not exclusive, but is not currently shared. An active session icon is visible.
Locked (normal)		Your administrator has configured the appliance to lock KVM and Virtual Media (VM) sessions together. You have a normal KVM session and have opened a VM session. Your KVM session cannot be shared or preempted, and it is not subject to inactivity time-out. It can be terminated by an administrator. For more information, see “Using virtual media” on page 49.
Exclusive		You have exclusive control over the target device. During this KVM session the connection to the target device cannot be shared, but it can be preempted or observed in stealth mode by an administrator.
Active sharing: (primary)		You are the first user to connect to the target device, and you have allowed other users to share the KVM session.
Active sharing: (secondary)		You can view and interact with the target device while sharing the KVM session with a primary user and, possibly, other secondary users.
Passive sharing		You can view the video ouput of the target device, but you are not allowed to have keyboard and mouse control over the target device.
Stealth		You can view the video output of the target device without the permission or knowledge of the primary user. You cannot have keyboard and mouse control over the target device. This session type is available for administrators only.
Scanning		You can monitor up to 16 target devices in thumbnail view. No status indicator icon is visible when in scan mode.

4.2 Using preemption

Preemption provides a means for users with sufficient privilege to take control of a target device from another user with lesser or equal privilege.

All users sharing the connection that is being preempted are warned, unless the target device is connected to a ServSelect III VM appliance. If the primary user has the corresponding access rights, they can reject the preemption.

Table outlines the preemption scenarios and detailed scenarios in which preemption requests can be rejected.

Preemption scenarios

Current user	Preempted by	Preemption can be rejected
User	Local user	No
User	User administrator	No
User	Appliance administrator	No
Appliance administrator	Local user	Yes
Appliance administrator	Appliance administrator	Yes
User administrator	Local user	No
User administrator	User administrator	Yes
User administrator	Appliance administrator	No
Local user	User administrator	Yes
Local user	Appliance administrator	Yes

Preemption of a user by an administrator

If an administrator attempts to access a target device that is being accessed by a user, a message requests that the administrator wait while the user is informed that their session will be preempted. The user cannot reject the preemption request and will be disconnected. If the target device is attached to a ServSelect III VM appliance, the user will not be warned. The time period given before disconnection is defined by the Video session preemption timeout setting in the **Global - Sessions** category. For information, see “Configuring Global Network settings” on page 70 and “Configuring Global Session settings” on page 71.

Preemption of a local user/administrator by an administrator

If an administrator attempts to access a target device that is being accessed by the local user or by another administrator with equal privileges, the currently connected user can accept or reject the preemption request. A message asks the connected local user or administrator whether they want to accept the preemption request. If the target device is attached to a ServSelect III VM appliance, the user will not be given the option to accept or reject preemption. If the preemption request is rejected, a message is displayed informing the administrator that their request has been rejected and that they cannot access the target device.

In scenarios where a preemption request can be rejected, the Session Preemption Request window opens. Use this window to accept the preemption request by clicking the **Accept** button, or reject the preemption request by clicking the **Reject** button or by closing the window.

To preempt the current user, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on the target device in the Unit list.
   - Select the target device, then click the **Connect Video** button.
   - Right-click on the target device. Select **Connect Video** from the pop-up menu.
   - Select the target device and press Enter.
3. When another user is viewing this target device, a message indicates that the target device is already involved in a KVM session.
   If the appliance has connection sharing enabled, you are given the option to share the session. For information about connection sharing, see "Using digital share mode" on page 37. If your access rights (as compared with those of the primary user) allow it, you are prompted to either share or preempt the existing session. If the option is available, select **Preempt**.
4. Complete one of the following steps:
   - Click **OK** or **Yes**. A preemption notification is sent to the primary user. Depending on your access rights, the primary user might be able to reject the preemption.
   - Click **No** to let the primary user retain the connection.
5. If the preemption completes, the Video Viewer of the target device session opens.

For more information about access levels, see "Managing local user accounts" on page 79.

You cannot preempt a local user who is in broadcast mode. See the corresponding *Installation and User's Guide* for the KV2116, KV4116, or ServSelect III VM appliance for additional information.

4.3 Using exclusive mode

When operating a video session in exclusive mode, you cannot receive any share requests from other users. However, administrators can choose to preempt (or terminate) the session or monitor the session in stealth mode.

You cannot use exclusive mode when connecting to a target device on a ServSelect III VM appliance.

To enable exclusive KVM sessions on an appliance, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on a KV2116 or KV4116 appliance in the Unit list.
   - Select a KV2116 or KV4116 appliance from the Unit list, then click the **Manage Appliance** button.
   - Right-click on a KV2116 or KV4116 appliance in the Unit list. Select **Manage Appliance** from the pop-up menu.
   - Select a KV2116 or KV4116 appliance in the Unit list and press Enter.
3. Click the **Settings** tab in the AMP.
4. Select the **Global - Sessions** subcategory.

5. Select the **Enable Shared** Sessions check box in the **Connection Sharing** area.
6. Select **Exclusive Connections** in the **Connection Sharing** area.

Only the primary user of a shared connection or the only user of a non-shared session can access the Video Viewer in exclusive mode. To access the Video Viewer in exclusive mode, complete the following steps:

1. Open a KVM session to a target device.
2. Select **Tools** > **Exclusive Mode** from the Video Viewer toolbar.
3. If the KVM session is currently shared, only the primary user can designate the session as exclusive. A message warns the primary user that secondary sessions will be terminated if an exclusive session is invoked.

   Complete one of the following steps:

   - Select **Yes** to terminate the sessions of the secondary users.
   - Select **No** to cancel the exclusive mode action.

Secondary users cannot share the exclusive KVM session. However, administrators or users with certain access rights can still terminate the session.

4.4 Using digital share mode

Multiple users can view and interact with a target device using digital share mode. When a session is shared, the secondary user can be an active user with keyboard and mouse control or a passive user that does not have keyboard and mouse control.

You cannot use digital share mode when connecting to a target device on a ServSelect III VM appliance.

To configure an appliance to share KVM sessions, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on a KV2116 or KV4116 appliance in the Unit list.
   - Select a KV2116 or KV4116 appliance from the Unit list, then click the **Manage Appliance** button.
   - Right-click on a KV2116 or KV4116 appliance in the Unit list. Select **Manage Appliance** from the pop-up menu.
   - Select a KV2116 or KV4116 appliance in the Unit list and press Enter.
3. Click the **Settings** tab in the AMP.
4. Select the **Global - Sessions** subcategory.
5. Select **Enable Share Mode** in the **Connection Sharing** area.
6. You can choose to select **Automatic Sharing**. This enables secondary users to automatically share a KVM session without first requesting permission from the primary user.

To share a digital connection, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on the target device in the Unit list.

- Select the target device, then click the **Connect Video** button.
- Right-click on the target device. Select **Connect Video** from the pop-up menu.
- Select the target device and press Enter.

3. When another user is viewing this target device, a message indicates that the target device is already involved in a KVM session.
   If connection sharing is enabled on the appliance and your access rights (as compared with those of the primary user) allow it, you are prompted to either share or preempt the existing session. If the option is available, select **Share**.
4. Complete one of the following steps:
   - Click **OK** or **Yes**. If Automatic Sharing is not enabled, a share request is sent to the primary user, who can accept the share request as either an active or passive (read-only) session, or reject the share request entirely.
   - Click **No** to cancel the share request.

If the primary user accepts the share request, or if Automatic Sharing is enabled, a KVM session to the target device session opens, and the session type icon within the new Video Viewer window indicates if the session status is active or passive. If the request is rejected, a message indicates that the request was denied. Administrators have several options at this point. They can either try to connect again and preempt the session or connect in stealth mode, or they can terminate the session entirely from the AMP **Active Sessions** category; see “Managing user sessions” on page 81.

If you are not prompted to connect in share mode, either the appliance to which the target device is connected is not configured to allow digital share mode sessions or it is not a KV2116 or KV4116 appliance.

4.5 Using stealth mode

Administrators can connect to a target device in stealth mode, viewing the video output of a remote user undetected. When in stealth mode, the administrator does not have keyboard or mouse control over the target device.

You cannot use stealth mode when connecting to a target device on a ServSelect III VM appliance.

To enable stealth KVM sessions on an appliance, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on a KV2116 or KV4116 appliance in the Unit list.
   - Select a KV2116 or KV4116 appliance from the Unit list, then click the **Manage Appliance** button.
   - Right-click on a KV2116 or KV4116 appliance in the Unit list. Select **Manage Appliance** from the pop-up menu.
   - Select a KV2116 or KV4116 appliance in the Unit list and press Enter.
3. Click the **Settings** tab in the AMP.
4. Select the **Global - Sessions** subcategory.
5. Select **Stealth Connections** in the **Connection Sharing** area.

To monitor a target device in stealth mode, complete the following steps:

1. Click the **Devices** button in the Explorer.
2. Complete one of the following steps:
   - Double-click on the target device in the Unit list.
   - Select the target device, then click the **Connect Video** button.
   - Right-click on the target device. Select **Connect Video** from the pop-up menu.
   - Select the target device and press Enter.
3. If another user is already viewing this target device, a message indicates that the target device is already involved in a KVM session.
   If connection sharing and stealth connections are enabled on the appliance and your access rights (as compared with those of the primary user) allow it, you are prompted to either share or preempt the existing session. If the option is available, select **Stealth**.
4. Complete one of the following steps:
   - Click **OK** or **Yes**.
   - Click **No** to cancel the stealth request.

A KVM session to the target device opens, and the administrator can view all video output of the target device while remaining undetected.

If Stealth is not listed as an option, one of the following conditions exist:

- the appliance to which the target device is connected is not configured to allow Stealth Connections
- you do not have the necessary access rights (Stealth permissions follow Preemption permissions)
- the appliance the target device is connected to is not a KV2116 or KV4116 appliance

4.6 Using scan mode

You can view multiple target devices using the scan mode Thumbnail Viewer. This view contains a series of thumbnail frames, each containing a small, scaled, non-interactive version of a target device screen image. The target device name and status indicator are visible below each thumbnail as follows:

- A green circle icon indicates that a target device is currently being scanned.
- A red X icon indicates that the last scan of the target device failed. The scan can have failed due to a credential or path failure (for example, the target device path on the appliance was not available). The tool tip for the icon indicates the reason for the failure.

You can set up a scan sequence of up to 16 target devices to monitor. The scan mode moves from one thumbnail image to the next, logging into a target device and displaying an updated target device image for a specified length of time (View Time Per Server), before logging out of that target device and moving on to the next thumbnail image. You can also specify a scan delay between thumbnails (Time Between Servers). During the delay, you can see the last thumbnail image for all target devices in the scan sequence, but you won't be logged into any target devices.

When you first open the Thumbnail Viewer, each frame is filled with a black background until a target device image is visible. An indicator icon at the bottom of each frame

displays the target device status. The default thumbnail size is based on the number of target devices in the scan list.

Scan mode has a lower priority than an active connection. If a user is connected to a target device, that target device is skipped in the scan sequence, and scan mode proceeds to the next target device. No login error messages are visible. After the interactive session is closed, the thumbnail is included in the scan sequence again.

You can disable a target device thumbnail from the scan sequence. The thumbnail image remains, but it is not updated until it is once again enabled.

Accessing scan mode

To access scan mode, complete the following steps:

1. Select the **Appliance**, **Devices**, **Sites**, or **Folders** button in the Explorer window.
2. Select two or more target devices in the Unit list by pressing the Shift or Control key. The **Scan Mode** button is visible.
3. Click the **Scan Mode** button. The Thumbnail Viewer window opens.

Setting scan options

To set scan preferences, complete the following steps:

1. Select **Options > Preferences** from the Thumbnail Viewer menu. The Preferences window opens.
2. In the **View Time Per Server** field, enter the time each thumbnail is active during the scan, in the range of 10 to 60 seconds.
3. In the **Time Between Servers** field, enter the time the scan stops between each target device, in the range of 5 to 60 seconds.
4. Click **OK**.

To change the thumbnail size, complete the following steps:

1. Select **Options > Thumbnail Size** from the Thumbnail Viewer menu.
2. Select a thumbnail size from the cascaded menu.

Managing the scan sequence

To pause or restart a scan sequence, complete the following steps:

1. Select **Options > Pause Scan** from the Thumbnail Viewer menu.
2. The scan sequence pauses at the current thumbnail if the Thumbnail Viewer has a scan in progress or restarts the scan if currently paused.

To disable a target device thumbnail in the scan sequence, complete one of the following steps:

- Select a target device thumbnail. Select **Thumbnail > "target device name" > Enable** from the Thumbnail Viewer menu. (The Enable menu item state can be toggled from checked (enabled) to unchecked (disabled) each time it is selected).
- Right-click on a target device thumbnail and select **Disable** from the pop-up menu.
  Updating of that thumbnail image stops until it is enabled again.

To enable a target device thumbnail in the scan sequence, complete one of the following steps:

- Select a target device thumbnail. Select **Thumbnail** > **"target device name"** > **Enable** from the Thumbnail Viewer menu. (The Enable menu item state can be toggled from checked (enabled) to unchecked (disabled) each time it is selected).
- Right-click on a target device thumbnail and select **Enable** from the pop-up menu.
  Updating of that thumbnail image resumes.

If a target device is currently being accessed by a user, the Enable Scan menu is disabled for that target device thumbnail.

Using the Thumbnail Viewer

To open a session to a target device from the Thumbnail Viewer, complete one of the following steps:

- Select a target device thumbnail. Select **Thumbnail** > **"target device name"** > **View Interactive Session** from the Thumbnail Viewer menu.
- Right-click on a target device thumbnail and select **View Interactive Session** from the Thumbnail Viewer menu.
- Double-click on a target device thumbnail.

That target device desktop opens in a Video Viewer window.

To set target device credentials from the Thumbnail Viewer, complete the following steps:

1. Complete one of the following steps:
   - Select a target device thumbnail. Select **Thumbnail** > **"target device name"** > **Credentials** from the Thumbnail Viewer menu.
   - Right-click on a target device thumbnail and select **Credentials** from the pop-up menu. The Login window opens.
   - Double-click the thumbnail window.
2. Enter a user name and password for the target device.

4.7 Window features

Figure 4-1 shows the Video Viewer window areas; descriptions follow in Table . The following figure shows one way of arranging buttons on the toolbar. You can customize the buttons and display position.

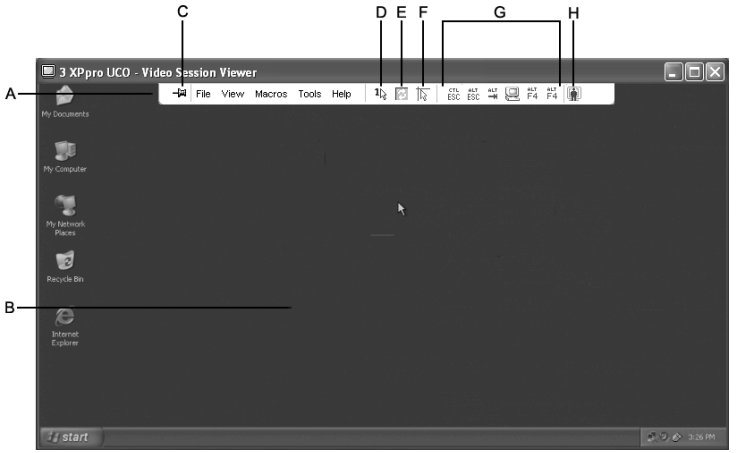

Figure 4-1. Video Viewer window

Video Viewer window areas

Area	Description
A	**Menu and toolbar:** Provides access to many of the features in the Video Viewer.
B	**Accessed target device desktop:** Interact with the target device through this window.
C	**Thumbtack button**: Determines toolbar position. When locked, the toolbar remains fixed on screen. When unlocked, the toolbar is visible only when the mouse hovers over the top of the window.
D	**Single Cursor Mode button:** Hides the local cursor and displays only the target device cursor.
E	**Refresh Video button:** Regenerates the digitized video image of the target device desktop.
F	**Align Local Cursor button:** Re-establishes true tracking of the local cursor to the target device cursor.
G	**User-selected buttons:** You can choose to display additional buttons and macro commands on the toolbar.
H	**Connection Status indicator:** Icons indicate the status of the KVM session. See Table for more information.

4.8 Adjusting the view

Using menus or buttons in the Video Viewer window, you can:

- Align the mouse cursors.
- Refresh the screen.
- Enable or disable full screen mode.
- Enable automatic or manual scaling of the session image. With automatic scaling, the desktop window remains fixed and the target device image is scaled to fit the window. With manual scaling, a drop-down menu of supported image scaling resolutions is visible.

To align the mouse cursors, click the Align Local Cursor button in the Video Viewer toolbar. The local cursor aligns with the cursor on the target device.

If cursors drift out of alignment, turn off mouse acceleration on the target device.

To refresh the screen, complete one of the following steps:

- Click the **Refresh Image** button in the Video Viewer toolbar.
- Select **View > Refresh** from the Video Viewer menu. The digitized video image is regenerated.

To enable full screen mode:

- If you are using Windows, click the **Maximize** button in the upper right corner of the window.
- Select **View > Full Screen** from the Video Viewer menu.

The desktop window is hidden and only the accessed target device desktop is visible. The screen is resized up to a maximum of 1024 x 768. If the desktop has a higher resolution, then a black background surrounds the full screen image. The floating toolbar is visible.

To disable full screen mode:

- Click the **Full Screen Mode** button on the floating toolbar to return to the desktop window.
- Select **View > Full Screen** from the Video Viewer menu.

To enable automatic or manual scaling, complete one of the following steps:

- To enable automatic scaling, select **View > Scaling > Auto Scale** from the Video Viewer menu. The target device image is scaled automatically.
- To enable manual scaling, select **View > Scaling** from the Video Viewer menu, then select the dimension to scale the window.

Additional video adjustment

Generally, the Video Viewer automatic adjustment features optimizes the video for the best possible view. However, you can fine tune the video with the help of technical support. Video adjustment is a global setting and applies to each target device you access.

NOTE:
The following video adjustments should be made only on the advice and with the help of technical support.

To manually adjust the video quality of the window, complete the following steps:

1. Select **Tools** > **Manual Video Adjust** from the Video Viewer menu. The Manual Video Adjust window opens. See Figure 4-2; descriptions follow the figure in Table .
2. Click the icon corresponding to the feature you want to adjust.
3. Move the slider bar and then fine tune the setting by clicking the **Min (-)** or **Max (+)** buttons to adjust the parameter for each icon pressed. The adjustments take effect immediately in the Video Viewer window.
4. When finished, click **Close** to exit the Manual Video Adjust window.

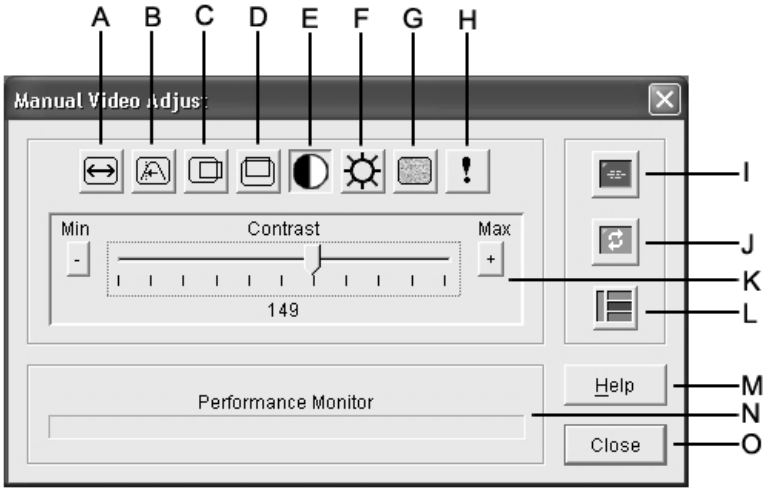

Figure 4-2. Manual Video Adjust window

Manual Video Adjust window areas

Area	Description	Area	Description
A	Image capture width	I	Automatic video adjustment
B	Pixel sampling fine adjust	J	Refresh image
C	Image capture horizontal position	K	Adjustment bar
D	Image capture vertical position	L	Video test pattern
E	Contrast	M	Help button
F	Brightness	N	Performance monitor
G	Noise threshold	O	Close button
H	Priority threshold		

4.9 Adjusting mouse options

The Video Viewer mouse options affect cursor type, scaling, alignment, and resetting. Mouse settings are device-specific; that is, they can be set differently for each target device.

NOTE: If the server does not support the ability to disconnect and reconnect the mouse (almost all newer PCs do), then the mouse will become disabled and the server will have to be rebooted.

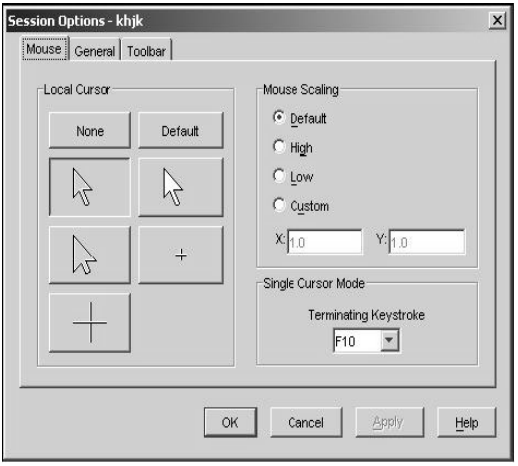

Figure 4-3. Viewer Mouse Session Options window

Cursor type

The Video Viewer offers five display choices for the local mouse cursor. You can also select no cursor or the default cursor.

To change the mouse cursor setting, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.
2. Click the **Mouse** tab.
3. Select a mouse cursor type in the **Local Cursor** area.
4. Click **OK**.

Scaling

You can select any of three preconfigured mouse scaling options or set custom scaling. The preconfigured settings are: Default (1:1), High (2:1) or Low (1:2), as follows:

- In a 1:1 scaling ratio, every mouse movement on the desktop window sends an equivalent mouse movement to the target device.
- In a 2:1 scaling ratio, the same mouse movement sends a 2X mouse movement.
- In a 1:2 scaling ratio, the value is 1/2X.

To set mouse scaling, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.

2. Click the **Mouse** tab.
3. To use one of the preconfigured settings, check the corresponding radio button in the **Mouse Scaling** area.
4. To set custom scaling, click the **Custom** radio button. The **X** and **Y** fields become enabled. Type a mouse scaling value in the **X** and **Y** fields. For every mouse input, the mouse movements are multiplied by the corresponding X and Y scaling factors. Valid input ranges are 0.25 to 3.00.

Single cursor mode

When using single cursor mode, the Video Viewer title bar will show the keystroke that should be pressed to exit this mode.

To change the terminating keystroke for single cursor mode, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.
2. Click the **Mouse** tab.
3. Select the desired terminating keystroke from the drop down list in the **Single Cursor Mode** area.
4. Click **OK**.

4.10 Adjusting general options

The General tab in the Session Options window allows you to control Keyboard Pass-through in non-full screen mode, Menu Activation Keystroke, and Background Refresh.

To adjust general options, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer menu. The Session Options window opens.
2. Click the **General** tab.
3. Select the **Keyboard Pass-through** check box to enable Keyboard Pass-through, or clear the check box to disable Keyboard Pass-through. The **Keyboard Pass-through** check box is not selected by default. When **Keyboard Pass-through** is selected, all keystrokes except for Control-Alt-Delete are sent directly to the target device instead of the client computer.
4. Select a keystroke to use to activate the Video Viewer toolbar from the list in the **Menu Activation Keystroke** area.
5. If you want the Video Viewer to receive a constant stream of video data from the target device, select the **Background Refresh** check box. If you want the Video Viewer to receive data only when a change has occurred on the target device, clear the **Background Refresh** check box.

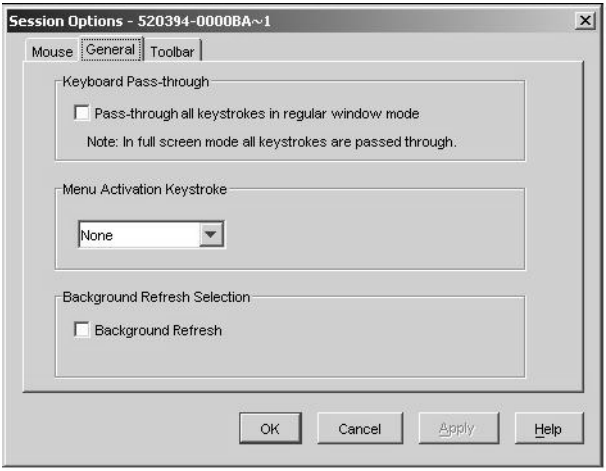

Figure 4-4. Session Options - General tab

4.11 Adjusting the Video Viewer toolbar

You may add up to 10 buttons to the toolbar. Use these buttons to provide easy access to defined function and keyboard macros. By default, the **Align Local Cursor**, **Refresh Image**, and **Single Cursor Mode** buttons are visible on the toolbar.

To add buttons to the toolbar, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer toolbar. The Session Options window opens.
2. Click the **Toolbar** tab.
3. Select the items you want to add to the Video Viewer toolbar.
4. Complete one of the following steps:
   - Click **OK** to accept the changes and return to the Video Viewer main window.
   - Click **X** or **Cancel** to return to Video Viewer main window without making changes.

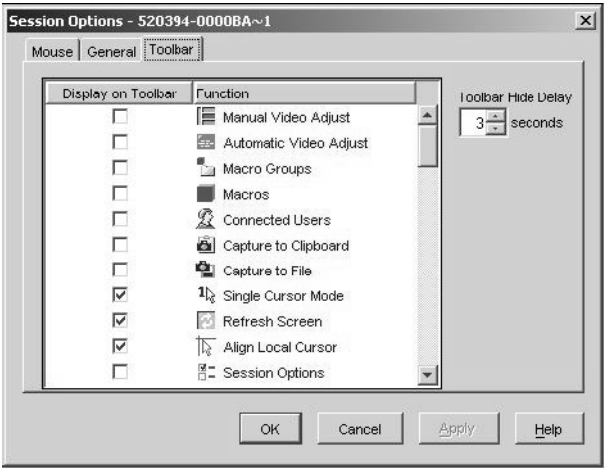

Figure 4-5. Session Options Window - Toolbar tab

Setting the Toolbar Hide Delay time

The toolbar disappears when you remove the mouse cursor unless the **Thumbtack** button has been clicked. You can change the interval between the removal of the mouse cursor and the disappearance of the toolbar by adjusting the Toolbar Hide Delay time.

To change the Toolbar Hide Delay time, complete the following steps:

1. Select **Tools > Session Options** from the Video Viewer toolbar. The Session Options window opens.
2. Click the **Toolbar** tab.
3. Complete one of the following steps:
   - In the **Toolbar Hide Delay** field, type the number of seconds you want the toolbar to be visible after the mouse cursor is removed.
   - Using the **Up** and **Down** buttons, click to increase or decrease the number of seconds you want the toolbar to be visible after the mouse cursor is removed.
4. Complete one of the following steps:
   - Click **OK** to accept the changes and return to the Video Viewer.
   - Click **X** or **Cancel** to return to Video Viewer without making changes.

4.12 Using macros

Use the Video Viewer macro function to:

- Send a macro from a predefined macro group. Macro groups for Windows and Sun are already defined. Selecting from the available categories and keystrokes saves time and eliminates the risk of typographical errors.
- Change the macro group that is listed by default. This causes the macros in the specified group to be available in the Video Viewer Macros menu.

Macro group selection are device-specific; that is, it can be set differently for each target device.

Sending macros

To send a macro, select Macros from the Video Viewer menu and choose a macro from the list.

Selecting the macro group to display

You can select the macro group applicable to the operating system of the target device.

To display macro groups in the Macros menu, complete the following steps:

1. Select **Macros > Display on Menu** from the Video Viewer menu.
2. Select the macro group you want to list on the Video Viewer Macro menu.
3. The macro group you select will be displayed in the Video Viewer Macros menu the next time you open the Macros menu.

4.13 Using virtual media

With virtual media you can map a physical drive on the local client machine as a virtual drive on a target device. You can also add and map an ISO or diskette image file on the local client as a virtual drive on the target device.

You can have one CD drive and one mass storage device mapped concurrently.

- A CD drive, DVD drive, or ISO disk image file is mapped as a virtual CD drive.
- A diskette drive, diskette image file, USB memory device, or other media type is mapped as a virtual mass storage device.

Requirements

Virtual media is supported on KV2116 and KV4116 appliances.

The target device must be connected to the KV2116 or KV4116 appliance with a VM SAM USB2-VGA cable.

The target device must support the types of USB2-compatible media that you virtually map. In other words, if the target device does not support a portable USB memory device, you cannot map the local device as a virtual media drive on the target device.

You (or the user group to which you belong) must have permission to establish virtual media sessions or reserved virtual media sessions to the target device.

A KV2116 will support up to three concurrent virtual media sessions (one local and two remote). A KV4116 will support up to four concurrent virtual media sessions (including local and remote). Only one virtual media session can be active to a target device at one time.

Sharing and preemption considerations

The KVM and virtual media sessions are separate; therefore, there are many options for sharing, reserving or preempting sessions.

For example, the KVM and virtual media sessions can be locked together. In this mode, when a KVM session is disconnected, so is the associated virtual media session. If the sessions are not locked together, the KVM session can be closed but the virtual media session remains active.

After a target device has an active virtual media session without an associated active KVM session, either the original user (User A) can reconnect or a different user (User B) can connect to that channel. You can set an option in the Virtual Media window (Reserved) that lets only User A access the associated target device with a KVM session.

If User B has access to that KVM session (the Reserved option is not enabled), User B could control the media that is being used in the virtual media session. In some environments, this might not be desirable.

By using the Reserved option in a tiered environment, only User A can access the lower appliance and the KVM channel between the upper appliance and lower appliance is reserved for User A.

Preemption levels offer additional flexibility of combinations.

Virtual Media window

Use the Virtual Media window to manage the mapping and unmapping of virtual media. The window displays all the physical drives on the client computer that can be mapped as virtual drives (non-USB hard drives are not available for mapping). You can also add ISO and diskette image files and then map them using the Virtual Media window.

After a target device is mapped, the Details View of the Virtual Media window displays information about the amount of data transferred and the time elapsed since the target device was mapped.

You can specify that the virtual media session is reserved. When a session is reserved, and the associated KVM session is closed, another user cannot open a KVM session to that target device. If a session is not reserved, another KVM session can be opened. Reserving the session can also be used to make sure that a critical update is not interrupted by another user attempting to preempt the KVM session or by inactivity time-outs on the KVM session.

You can also reset the VM SAM USB2-VGA cable from the Virtual Media window. This action resets every form of USB media on the target device, and should therefore be used with caution, and only when the target device is not responding.

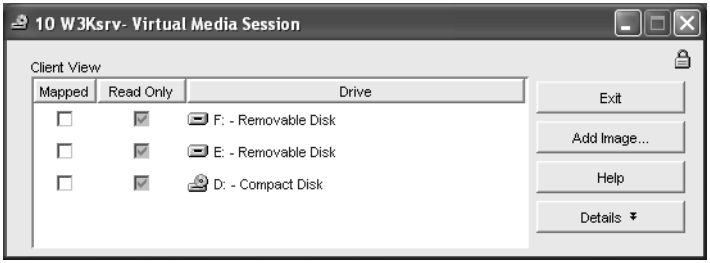

Figure 4-6. Virtual Media window

Virtual media session settings

Virtual media session settings include locking, mapped drives access mode, and encryption level. See “Configuring Global Virtual Media settings” on page 72 to specify these settings for the supported KV2116 or KV4116 appliances.

Table lists and describes the virtual media session settings.

Virtual media session settings

Setting	Description
Locked	The Locked setting specifies whether a virtual media session is locked to the KVM session on the target device. When locking is enabled (which is the default) and the KVM session is closed, the virtual media session also closes. When locking is disabled and the KVM session is closed, the virtual media session remains active.
Mapped drives access mode	You can set the access mode for mapped drives to read-only. When the access mode is read-only, you cannot write data to the mapped drive on the client computer. When the access mode is not set as read-only, you can read and write data from or to the mapped drive. If the mapped drive is read-only by design (for example, certain CD drives, DVD drives, or ISO images), the configured read-write access mode is ignored. Setting the read-only mode can be helpful when a read-write drive such as a mass storage device or a USB removable media is mapped, and you want to prevent the user from writing data to it.
Encryption level	You can configure up to three encryption levels for virtual media sessions. Any combination is valid. The choices are: DES, 3DES and 128-bit SSL. The highest level selected is used. The default is no encryption (no encryption levels selected).

Opening a virtual media session

The following procedures are valid only on KV2116 or KV4116 appliances that are connected with VM SAM USB2-VGA cables.

To open a virtual media session, complete the following steps:

1. Open a Video Viewer session to the target device.
2. From the Video Viewer toolbar, select **Tools > Virtual Media**. The Virtual Media window opens.
3. If you want to make this a reserved session, on the Virtual Media window click **Details,** then select the **Reserved** check box.

Mapping virtual media drives

To map a virtual media drives, complete the following steps:

1. Open a virtual media session from the Video Viewer toolbar by selecting **Tools > Virtual Media.**
2. To map a physical drive as a virtual media drive, complete the following steps:
   a. In the Virtual Media window, select the **Mapped** check box next to the drive or drives you want to map.
   b. If you want to limit the mapped drive to read-only access, select the **Read Only** check box next to the drive prior to mapping the drive. If the virtual media

session settings were previously configured so that all mapped drives must be read-only, this check box is already enabled and cannot be changed.

You might want to select the **Read Only** check box if the session settings enabled read and write access, but you want to limit the access of a particular drive to read-only.

3. To add and map an ISO or diskette image as a virtual media drive, complete the following steps:
   a. In the Virtual Media window, click **Add Image**.
   b. The Common File Chooser window opens, with the directory containing disk image files (ending in .iso or .img) visible. Select an ISO or diskette image file and click **Open**.
   c. The file header is checked to make sure it is correct. If it is, the Common File Chooser window closes and the chosen image file opens in the Virtual Media window, where it can be mapped by selecting the **Mapped** check box.
   d. Repeat steps a through c for any additional ISO or diskette images you want to add. You can add any number of image files (up to the limits imposed by memory), but you can only have one virtual CD or virtual mass storage mapped concurrently.

   If you attempt to map too many drives (one CD and one mass storage device) or too many drives of a particular type (more than one CD or mass storage device), a message is displayed. If you still want to map a new drive, you must first unmap an existing mapped drive, then map the new drive.

   After a physical drive or image is mapped, it can be used on the target device.

To unmap a virtual media drive, eject the mapped drive from the target device. Clear the Mapped check box.

Displaying virtual media drive details

To display virtual media drive details, complete the following steps:

1. In the Virtual Media window, click **Details**. The window expands to display the Details table. Each row indicates:
   - **Target Drive** - Name used for the mapped drive, such as Virtual CD 1 or Virtual CD 2.
   - **Mapped to** - Identical to Drive information that is listed in the Client View Drive column.
   - **Read Bytes and Write Bytes** - Amount of data transferred since the mapping.
   - **Duration** - Elapsed time since the drive was mapped.
2. To close the Details view, click **Details** again.

Resetting USB media devices

To reset all USB media devices on the target device, complete the following steps:

Important: The USB reset feature resets every USB device on the target device, including the mouse and keyboard. It should only be used when the target device is not responding.

1. In the Virtual Media window, click **Details**.
2. The Details View is visible. Click **USB Reset**.

3. A warning message indicates the possible effects of the reset. Click **Yes** to confirm the reset or **No** to cancel the reset.
4. To close the Details view, click **Details** again.

Closing a virtual media session

To close the Virtual Media window, complete the following steps:

1. Click **Exit** or **X** to close the window.
2. If you have any mapped drives, a message indicates that the drives will be unmapped. Click **Yes** to confirm and close the window or click **No** to cancel the close.

If you attempt to disconnect an active KVM session that has an associated locked virtual media session, a confirmation message indicates that any virtual media mappings will be lost.

See “Sharing and preemption considerations” on page 49 for information about other factors that can affect virtual media session closings.

5. Serial Console Viewer

5.1 About the Serial Console Viewer

The ServSelect IP Software built-in Serial Console Viewer is a Telnet client that allows you to establish serial sessions with servers attached to SCPS appliances. You may tailor user preferences for all sessions, as well as session properties for each server. The Serial Console Viewer offers a separate history mode to review session data, a scripting function for automatic server login and a logging function for saving session data to a file.

When launching a Serial Console Viewer session to an SCPS server, ServSelect IP Software may use either an SSH or plain text (non-encrypted) session, depending on the settings of the SCPS appliance. The SCPS may be set to support SSH sessions only, plain text sessions only or both types of sessions at the same time.

When the SCPS is set to support both types of sessions, the Encryption Method dialog box is displayed; you may then choose a session type and optionally save your choice for use in future Serial Console Viewer sessions. When an SSH connection is initiated, the Serial Console Viewer is launched on top of an SSH tunnel. SSH settings are configured in the SCPS AMP.

To access the Serial Console Viewer:

1. Click the *Servers* tab in the ServSelect IP Software Explorer.
2. Double-click on the server in the Unit list.

-or-

Select the server, then click the *Connect Serial* task button.

-or-

Right-click on the server. Select *Connect Serial* from the pop-up menu.

-or-

Select the server and press **Enter**.

3. If the SCPS is confi gured to allow either SSH or plain text connections, the Encryption Method dialog box appears. Enable the *Keep choice as default setting* checkbox if you wish for the selection you make to be maintained for subsequent launch requests during the current ServSelect IP Software session. When this checkbox is enabled, the Encryption Method dialog box will not reappear during the current ServSelect IP Software session unless login credentials are cleared by selecting *Tools - Clear Login Credentials* from the ServSelect IP Software Explorer menu. When this checkbox is disabled, the Encryption Method dialog box will be displayed each time the Serial Console Viewer is launched.
4. Click *Yes* to launch the Serial Console Viewer using an SSH tunnel.

-or-

Click *No* to launch the Serial Console Viewer in plain text mode.

The Viewer launches in a new window.

To close a Serial Console Viewer session:

Select *File - Exit* from the Serial Console Viewer menu.

5.2 Window Features

Figure 5-1 shows the Serial Console Viewer window areas, and descriptions follow.

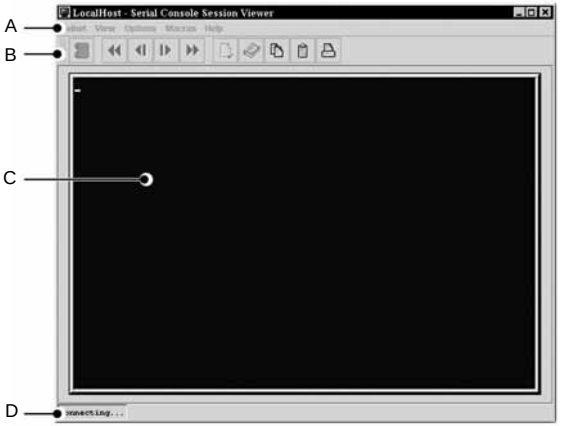

Figure 5-1. Serial Console Viewer Window

Serial Console Viewer Window Areas

Area	Description
A	**Menu bar:** Accesses many of the features of the Serial Console Window
B	**Toolbar:** Provides button equivalents to many menu commands
C	**Virtual terminal window:** Displays unit session data
D	**Status bar:** Indicates current session status

5.3 About Options

The Serial Console Viewer options allow you to:

- Customize global preferences for the Serial Console Viewer, that is, settings that all sessions will use.
- Customize individual server session properties. These settings are server-specific. They may be set differently for each server.
- Use the logging feature to save session data to a file.
- Copy, paste and print the screen contents to and from other applications.

5.4 Customizing Preferences

Preferences are used for all sessions. There are three types of preferences:

- Prompt on exit - When the exit warning prompt is enabled, a message appears when you try to exit the session. You may then choose to exit or continue the session. When disabled, the session closes without confirmation.
- Colors - The Colors preferences specify the background and text colors for the virtual terminal window during normal session operations (normal mode).
- Caret - The Caret preference indicates whether the cursor appears as an underline or as a block.

To customize preferences:

1. Select *Options - Preferences* from the Serial Console Viewer menu. The Preferences dialog box appears.
2. Enable or disable the *Prompt on exit* checkbox to indicate if users should be prompted to verify a request to exit the session. The default is enabled.
3. To change the background and text colors for the virtual terminal window during normal session operations:
   a. Click the *Background/Normal Mode* box and choose a color. The default value is white.
   b. Click the *Text/Normal Mode* box and choose a color. The default value is blue.
4. Click *OK* to save the changes and exit the dialog box.

-or-

Click *Cancel* to exit without saving any changes.

5.5 Customizing Session Properties

Session properties are set on a per-server basis. There are three session properties tabs: Terminal, Login Scripts and Logging.

Terminal settings

Terminal properties include:

- Virtual terminal window size.
- Terminal emulation type: ASCII, VT52, VT100, VT100+, VT102, VT220 or VT320.
- The terminal type used during Telnet session negotiation.
- Sequences to send for each of the **Arrow** keys.
- New line mode. This property enables or disables the automatic insertion of a line after each line of data. This is useful when connecting to servers that do not insert a carriage return in incoming or outgoing data, and prevents overwriting data when a new line is received.
- Auto line wrap. This property enables or disables wrapping characters onto the next line when a new character is received and the cursor is at the end of the line. When disabled, new characters will overwrite the last character on the line when the cursor is at the end of the line.
- Local echo. This property enables or disables the repeating of typed text. When you are connected to a server that does not repeat or echo the data you type, enabling local echo displays the typed text. However, if your server echoes data, enabling local echo will cause all typed data to appear twice.

- Strip 8th bit. This property enables or disables 7-bit ASCII. When enabled and you are connected to a server that requires 7-bit ASCII transmission, the eighth bit of every character sent and received will be stripped.
- History buffer size. This property specifi es the maximum number of lines that the history buffer can hold.
- Macro group. This option specifi es the macro group to be used during a server session. The macros in the specifi ed group will appear in the Macro menu.

Login Scripts

The Login Scripts tab contains the dialog box for enabling/disabling and editing automatic login scripts. See *Using Login Scripts* in this chapter for more information.

Logging

The Logging tab enables or disables automatic logging during the next server session. See *Using Logging* in this chapter for more information.

To customize terminal session properties:

1. Select *Options - Sessions Properties* from the Serial Console Viewer menu.

-or-

Click the *Session Settings* icon in the toolbar.

2. Click the *Terminal* tab.
3. In the Rows and Columns pulldown menus, select the number of rows and columns. The default value is 24 rows and 80 columns.
4. From the Terminal Emulation pulldown menu, select *ASCII*, *VT52*, *VT100*, *VT100+*, *VT102*, *VT220* or *VT320*. The default value is VT102.
5. The value in the Terminal Type field must exactly match what the unit's Telnet server expects. See the appliance or server documentation for requirements. The default value is ANSI.
6. From the Arrow Keys pulldown menu, select *VT100* or *ANSI*. (This field is valid only if the terminal emulation is not ASCII.) The default value is VT100.
7. From the Macro Group pulldown menu, select a group name or *All*. The default value is All (all macros will be available).
8. Enable or disable the *New Line Mode - Inbound* checkbox. When enabled, an inbound carriage return from the server is treated as if both a carriage return and a linefeed were received. When disabled, a linefeed is not added to an inbound carriage return. The default value is disabled.
9. Enable or disable the *New Line Mode - Outbound* checkbox. When enabled, an outbound carriage return to the server is always followed by a linefeed character. When disabled, a linefeed is not sent with a carriage return. The default value is disabled.
10. Enable or disable the *Auto Wrap Line* checkbox. The default value is enabled.
11. Enable or disable the *Local Echo* checkbox. When enabled, typed characters are echoed to the virtual terminal window; when disabled, they are not. The default value is disabled.

12. Enable or disable the *Strip 8th bit* checkbox. When enabled, the eighth bit of every character sent and received is stripped; when disabled, it is not. The default value is disabled.
13. Click *OK* to exit the dialog box and save any changes.

-or-

Click *Cancel* to exit the dialog box without saving any changes.

5.6 Using Login Scripts

The Serial Console Viewer has a login script function that allows you to automatically log in to a server. A login script contains a sequence of Expect and Send strings, and initial transmission characters that work with them. A login script's definition mayalso contain the strings that indicate a successful and a failed login.

To use a login script, you must enable automatic login in a server's Session Properties dialog box (the default value is enabled).

ServSelect IP Software contains a default login script for supported appliances. When a Serial Console Viewer Telnet session is initiated to a supported unit, the default login script is run automatically. If the login is successful (that is, the string defined to indicate success is received), the session continues. If the login is not successful (that is, the string defined to indicate failure is received), the user is prompted for login credentials.

You may use the default login script, customize the default login script or create an entirely different login script. If you customize the default login script and later decide to return to the original, you may easily restore the default script content.

When you build the login script, you specify the Initial Character to be sent to the unit as soon as the Telnet session is established. The first Expect string indicates what the unit will send as its first prompt. The first Send string indicates what the login script will send to the unit after it receives the first Expect string.

You may build additional Expect and Send strings according to what the particular server will prompt for and what will be sent in response.

Changing a default login script

You may change a server's default login script in its Session Properties dialog box. When you click the *Login Scripts* tab, all the information from the current login script is displayed, including the Initial Character to be transmitted, the Send and Expect strings, the string that indicates success and the string that indicates failure. You may change the content of the existing fields, and you may add additional Send and Expect strings, up to the maximum allowed.

When a login script needs debugging, you may enable a property or option in the ServSelect IP Software Explorer that will open the Serial Console Viewer Telnet window before any login to the server is attempted. After the login script is successfully debugged, you may disable this feature, and the Telnet window will only open after a successful login.

To enable or disable automatic login:

1. Select *Options - Sessions Properties* from the Serial Console Viewer menu.

-or-

Click the *Session Settings* icon in the toolbar.

2. Click the *Login Scripts* tab.
3. Enable or disable the *Automate Login* checkbox. The default value is enabled. When automatic login is enabled, the login script must contain Success and Failure strings.
4. Click *OK* to exit the dialog box and save any changes.

-or-

Click *Cancel* to exit the dialog box without saving any changes.

To change a default login script:

1. Select *Options - Sessions Properties* from the Serial Console Viewer menu.

-or-

Click the *Session Settings* icon in the toolbar.

2. Click the *Login Scripts* tab.
3. In the Default Login Timeout field, enter the number of seconds the Serial Console Viewer will wait for a valid response to automatic login information, in the range 1-99999. The default value is 30 seconds.
4. In the Initial Character pulldown menu, select: *CR* (carriage return), *CR+LF* (carriage return and linefeed), *CR+CR* (carriage return and carriage return), *ESC* (Escape), *CTRL+P* (Control+P sequence, 0x10 in hex) or *None* (no initial transmission character). The default value is None.
5. In the first Expect field, type the 1-32 alphanumeric character string that you expect from the unit. Spaces are allowed. The SCPS Default Values table lists those appliances' default values.
6. In the first Send field, type the 0-32 alphanumeric character string to be sent in response to the Expect string. Spaces are allowed, and a blank field is valid. A CR or CR+LF is appended to the string, based on the New Line Mode - Outbound setting. If a Send field contains an entry, the Expect field cannot be blank. The SCPS Default Values table lists those appliances' default values.

You may use the following macros in the field. ServSelect IP Software will automatically replace these variables when the login script runs.

Macro	Will be replaced with
%I	IP address
%P	Port number
%U	Username
%W	Password

7. Enter additional Expect and Send field entries as needed, to a maximum of four each. The SCPS Default Values table lists those appliances' default values.

8. In the Success String field, enter the string that will indicate the login was successful. This field must contain a value when automatic login is enabled. The SCPS Default Values table lists those appliances' default values.
9. In the Failure String field, enter the string that will indicate the login was unsuccessful. This field must contain a value when automatic login is enabled. The SCPS Default Values table lists those appliances' default values.
10. Enable or disable the *Reset to Default* checkbox to reset the login script to its default content. The default value is disabled.
11. Click *OK* to exit the dialog box and save any changes.

-or-

Click *Cancel* to exit the dialog box without saving any changes.

SCPS Default Values

Field	Default Value
Initial Character	None
First Expect	Username:
First Send	%U
Second Expect	Password
Second Send	%W
Success String	Authentification Complete
Failure String	Invaild Login

To enable or disable debug mode for login scripts:

You may enable or disable debug mode for login scripts in the ServSelect IP Software Explorer options or in a server's properties.

To access the enable/disable debug mode option, select *Tools - Options* from the ServSelect IP Software Explorer menu.

-or

1. To access the enable/disable debug mode property:
   a. Select an appliance or server in the Unit list.
   b. Select *View - Properties* from the ServSelect IP Software Explorer menu.

-or-

Click the *Properties* task button.

-or-

Right-click on the unit. Select *Properties* from the pop-up menu. The Properties dialog box appears.

2. Click the *Telnet* tab.

3. Enable/disable the *Open Window before login* checkbox. When enabled, the Serial Console Viewer Telnet window will open before login is attempted. When disabled, the Telnet window will open only after a successful login.
4. Click *OK* to save the new setting.

-or-

Click *Cancel* to exit without saving the new setting.

5.7 Using Macros

- The Serial Console Viewer macro function allows you to:
- Send multiple keystrokes to a server, including keystrokes that you cannot generate without affecting your local system, such as **Control-Alt-Delete**.
- Create, edit and delete macros. You may also defi ne a hotkey for a macro that, when entered, will run the macro. This is an alternative to using a menu selection to run the macro.
- Create, edit and delete macro groups.
- Change the macro group that will appear in the Macros menu. This causes the macros in the specifi ed group to be available in that menu. Alternatively, you may specify that all defi ned macros be available, rather than just those in one group. Macro group settings are server-specific. They may be set differently for each server.

To send a macro:

Select *Macros* - <*macro name*> from the Serial Console Viewer menu.

-or-

If the macro has a hotkey defined, enter the hotkey character(s) on your keyboard.

-or-

Select *Macros* - *Configure* from the Serial Console Viewer menu. The Macros dialog box appears. Select the desired macro from the Defined Macros list and then click the *Run* button.

Creating or editing a macro

To create and/or edit a macro:

1. Select *Macros* - *Confi gure* - *Macros* from the Serial Console Viewer menu. The Macros dialog box appears.
2. To create a macro, click the *Create* button.

-or-

To edit a macro, select it and click the *Edit* button. The Create Macro/Edit Macro dialog box appears.

3. If you are creating a macro, type a 1-32 character name in the Name field.
4. To define a hotkey for the macro, choose one from the Key pulldown menu. To add a modifier to the hotkey, enable the *Control*, *Shift* or *Alt* checkbox.
5. By default, the Include in Menu checkbox is enabled, indicating the macro will appear in the Macros menu (if it is a member of the macro group that is selected for inclusion in the menu). To exclude the macro from the Macros menu, disable this checkbox. In this case, if the macro's definition includes a hotkey, you will still be

able to use the hotkey to run the macro, even if the macro's name does not appear in the Macros menu.

6. In the Enter Keystrokes field, type the macro string. You may include the following special control characters:

\n = Newline	\b = Backspace
\r = Carriage return	\d = Delay character (500 milliseconds)
\f = Form feed	\0x?? = ?? is hexadecimal value
\t = Horizontal tab \	0??? = ??? is octal value

You may also insert a Telnet break sequence by selecting *Send Telnet Break* from the Control Code pulldown menu next to the Enter Keystrokes field.

7. Click *OK* to save the new information and return to the Macros dialog box. The newly created macro appears in the Defi ned Macros list
   -or
   Click *Cancel* to return to the Macros dialog box without saving any changes.
8. Click *Close*.

To delete a macro:

1. Select *Macros - Confi gure - Macros* from the Serial Console Viewer menu. The Macros dialog box appears.
2. Select the macro from the Defi ned Macros list. Click the *Delete* button. You are prompted to confi rm the deletion.
3. Click *Yes* to confi rm or *No* to cancel the deletion. You are returned to the Macros dialog box.
4. Click *Close*.

To create a macro group:

1. Select *Macros - Confi gure - Groups* from the Serial Console Viewer menu.
2. Click *Create*. The Create Macro/Edit Macro dialog box appears.
3. In the Macro Groups panel, click *Create*. A new row appears in the Macro Groups table.
4. Position the cursor in the Group Name column of the new row and enter the new group name. Duplicate macro group names are not allowed. Press **Enter**.
5. Click *OK* to save the new information and return to the Macros dialog box.

-or-

Click *Cancel* to return to the Macros dialog box without saving any changes.

6. Click *Close*.

To delete a macro group:

1. Select *Macros - Configure* from the Serial Console Viewer menu.
2. Select the macro group name in the Group Names list. To select multiple macro group names, press the **Shift** key while clicking.
3. Click the *Delete* button. You are prompted to confi rm the deletion.
4. Click *Yes* to confi rm or *No* to cancel the deletion. You are returned to the Macros dialog box.
5. Click *Close*.

To specify the macro group to appear in the Macros menu:

1. Select *Macros - Confi gure - Macros* from the Serial Console Viewer menu.

-or-

Click the *Session Settings* icon in the toolbar.

2. Select the Macro Group name that appears in the Macros menu and click *Edit*.
3. Click the Active and Active Group check boxes.
4. Click OK to exit.

Macros in the selected group will appear in the Macros menu.

Keep in mind that if a macro's definition has the Include in Macro Menu checkbox disabled, that macro will not appear in the menu, even if belongs to an enabled group; however, if the macro's definition includes a hotkey, it may be used to run the macro.

5.8 Using Logging

The Serial Console Viewer has a logging function that saves the contents of a session to a file. You may enable automatic logging or dynamically start logging at any time. Additionally, you may pause, resume and stop logging, regardless of whether it was started automatically or dynamically.

While logging is occurring or when it is paused, the status bar at the bottom of the Serial Console Viewer window contains a logging status label.

NOTE:
When you enable/disable automatic logging, the logging will begin or end at the start of the next. Serial Console Viewer session to that unit. If you change the default log file directory used for automatic logging, the change does not take effect until the next session to that unit.

The format of log file names is shown below, where <mmddyy> represents the month, day and year, and <hhmmss> represents the current hour, minute and second in military time.

scvTelnet<mmddyy>_<hhmmss>.log

The default log directory is session-specific. Each Serial Console Viewer session may have its own location for storing log files. You may change the name of the file and the location of the directory that stores the log files. If you do not change the default directory, log files are stored in a directory under the client software directory in your home directory.

You may view a log file at any time, using a standard text editor. The screen buffer is written to the log file when the buffer is full, or when logging is paused or stopped. To ensure the log file is up-to-date, either pause or stop the logging.

To enable or disable automatic logging:

1. Select *Options - Session Properties* from the Serial Console Viewer menu.

- or -

Click the *Session Settings* icon in the toolbar.

2. Click the *Logging* tab.
3. Enable or disable the *Logging* checkbox. The default value is disabled.
4. When you enable logging, the Default Directory field displays the current default location for log files. If that is the desired directory, click *OK*. To change the default log file directory, see *To change the default log file directory* in this chapter.

Automatic logging will start or stop when you initiate the next Serial Console

Viewer session to that server. When logging starts, the logging status label will indicate *Logging*.

To change the default log file directory:

1. Select *Options - Session Properties* from the Serial Console Viewer menu.

- or -

Select the *Session Settings* icon in the toolbar.

2. Click the *Logging* tab. The Default Directory field displays the current default location for log files.
3. Click the *Browse* button. The Set Directory dialog box appears.
4. Select a directory from the Look in list box.

- or -

Create a new directory:

   a. Click the *Create New Folder* button. A new directory named New Folder appears in the directory list.
   b. Click the *New Folder* entry in the directory list to highlight it. Then, click the entry again to edit its name. Type in a new name. Press **Enter**. The directory appears in alphabetical order in the directory list.
   c. Select the newly-created directory in the directory list. The File name field will now contain the name of the new directory.

5. Click the *Set Directory* button to select the newly-created or selected directory as the default log file directory. The Set Directory dialog box will close.
6. The Default Directory field now contains the name of the newly-created or selected directory. Click *OK* to save the new information.

- or -

Click *Cancel* to exit the dialog box without saving any new information.

To start dynamic logging:

1. Select *Options - Logging - Start* from the Serial Console Viewer menu. The Log dialog box appears.
2. The Look in list box contains the default log file directory and the File name field contains the default log file name. Using this file name format is recommended; however, you may change it for the duration of this session. If you choose to use the default log file name, skip to step 4.
3. To change the default log file name for the duration of the dynamic logging session, you may select a directory from the Look in pulldown menu. The directory list may contain directories and files. To create a new directory:

   a. Click the *Create New Folder* button. A new directory named New Folder appears in the directory list.
   b. Click the *New Folder* entry in the directory list to highlight it. Then click the entry again to edit its name. Type a new name. Press **Enter**. The directory appears in alphabetical order in the directory list.
   c. Double-click the newly-created directory in the directory list. The File name field will now contain the name of the new directory.

d. Type a new file name in the File name field. If you enter a file name that already exists, the new file will overwrite the old file.

4. Click *Log* to confi rm the directory selection and begin logging.

- or -

Click *Cancel* to exit the dialog box and cancel the request to start logging. When logging begins, the logging status label will indicate *Logging.*

To pause logging:

Select *Options - Logging - Pause* from the Serial Console Viewer menu. The logging status label will indicate *Logging Paused*.

To resume logging:

Select *Options - Logging - Resume* from the Serial Console Viewer menu. The logging status label will indicate *Logging*.

To stop logging:

Select *Options - Logging - Stop* from the Serial Console Viewer menu. The logging status label will disappear.

5.9 Moving Session Data

During a Serial Console Viewer session, you may:

- Copy a screen of session data to the system clipboard
- Copy the history buffer contents to the system clipboard
- Paste the contents of the system clipboard into a session
- Print a screen of regular session

Information that is copied from a session may be pasted in other applications. Similarly, information copied from other applications may be pasted into a Serial Console Viewer session.

NOTE:
Only textual (ASCII) data may be copied and pasted.

To copy a session screen:

Select *Edit - Copy Screen* from the Serial Console Viewer menu.

-or-

Click the *Copy Screen* icon in the toolbar.

The screen contents are saved to the system clipboard. You may then paste the clipboard contents into this or another application.

To copy session history data:

1. Select *Options - Copy Screen* from the Serial Console Viewer menu.

-or-

Click the *Copy Screen* icon in the toolbar.

The entire contents of the history buffer are copied to the system clipboard. You may then paste the clipboard contents into this or another application.

NOTE:
The entire history buffer is copied, regardless of the amount of data in it.

To paste system clipboard contents:

1. Place textual data on the system clipboard, using a text editor or other application.
2. Initiate a Serial Console Viewer session.
3. At the point where the clipboard contents should be pasted, select *Options* - *Paste* from the Serial Console Viewer menu.

-or-

Click the *Paste* icon in the toolbar.

To print a session screen:

1. Select *File* - *Print Screen* from the Serial Console Viewer menu.

-or-

Click the *Print Screen* icon in the toolbar.

2. The operating system's print dialog box appears. Make the appropriate settings. The screen contents will then be sent to the printer.

6. Appliance Management Panel

6.1 About the Appliance Management Panel

After you add an appliance in the software, you can view and configure unit parameters, view and control active video sessions, and execute a variety of control functions. These operations are accomplished through the Appliance Management Panel (AMP).

The AMP has three tabs: **Settings**, **Status**, and **Tools**, as follows:

- The **Settings** tab contains categories in the left portion of the tab. Categories with a preceding plus sign (+) have subcategories. The content of the remaining area of the panel changes according to the category or subcategory that is selected.

  Settings categories include general appliance information, user accounts, SNMP, and other unit configuration information.
- The **Status** tab displays information about currently active Video Viewer and virtual media sessions. As an administrator, you can disconnect sessions from this tab.
- The **Tools** tab can be used to execute control functions on the appliance such as rebooting, saving and restoring databases, and upgrading firmware.

Some operations that you perform through the AMP trigger a message indicating that a reboot is required in order for the change to take effect. In such cases, you can choose to reboot immediately or wait to reboot later.

You can use the AMP to manage KV2116, KV4116, or ServSelect III VM appliances. Some features are only available for KV4116 and KV2116 appliances.

NOTE: References to the local user refer to an OSD user connected to the appliance at the local user port.

For more information about the appliance and its operations, see the corresponding *Installation and User's Guide*.

To access the AMP, complete the following steps:

1. Click the **Appliances** button in the Explorer.
2. Complete one of the following steps
   - Double-click on an appliance in the Unit list.
   - Select an appliance from the Unit list, then click the **Manage Appliance** button.
   - Right-click on a KV2116, KV4116, or ServSelect III VM appliance in the Unit list. Select **Manage Appliance** from the pop-up menu.
   - Select an appliance in the Unit list and press Enter.
3. If this is the first time a unit has been accessed since the ServSelect IP Software was started, a user name and password prompt opens.
   a. Type in your user name and password. [If this is the first appliance access since initialization or reinitialization, the default user name is Admin (case sensitive) with no password.]
   b. Click **OK** to log in, or click **Cancel** to exit without logging in.

The AMP opens.

To exit the AMP, complete one of the following steps:

- Click **OK** to save any changes and exit the AMP.

- Click **Cancel** to exit the AMP without saving any changes.

6.2 Managing Global settings

The Global category lists the appliance product type, its serial number, and the language the appliance is currently using. Use the Global category to control many of the options for target devices running the software.

Configuring Global Network settings

The **Global - Network** subcategory specifies the IP address, subnet mask and gateway (all read-only if DHCP is enabled), MAC address (read-only), LAN interface speed, and DHCP state (enabled or disabled) of the appliance. The appliance name is also listed. The name is read-only in this sub-category; you can change the appliance name in the SNMP category.

To change global network values, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Global - Network** subcategory.

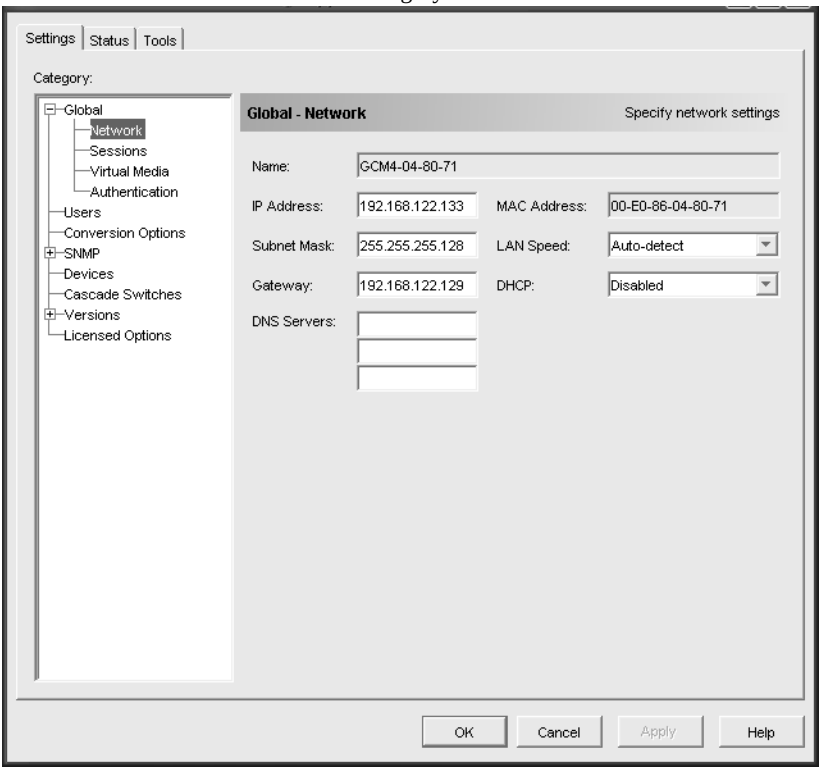

Figure 6-1. AMP Global Network settings

3. In the **DCHP** field, select **Disabled** or **Enabled** from the pull-down menu. When enabled, the appliance gets its IP address dynamically at boot time from a

DCHP server so the **IP Address**, **Subnet Mask**, **Gateway** fields and DNS servers are disabled.

4. In the **IP Address** field, enter the appliance address in IP dot notation. The value cannot be a loopback address or all zeros. This field can be modified only if DCHP is disabled.
5. In the **Subnet Mask** field, enter the appliance subnet mask in IP address dot notation. The value cannot be a loopback address or all zeros. This field can be modified only if DCHP is disabled.
6. In the **Gateway** field, enter the appliance gateway address in IP address dot notation. The value cannot be a loopback address. If there is no gateway address, enter 0.0.0.0. This field can only be modified if DCHP is disabled.
7. In the **LAN Speed** field, select a value from the pull-down menu.
8. If LDAP is licensed for the appliance, you can enter the IP address for up to three DNS target devices. If you are using a ServSelect III VM appliance, you can only enable DNS target devices through the serial interface of the appliance. See the corresponding KV2116, KV4116, or ServSelect III VM *Installation and User's Guide* for more information.
9. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

Configuring Global Session settings

Use the **Global - Sessions** subcategory to designate video session settings for the appliance, including Inactivity Time-out, Preemption Time-out, Encryption Levels, and Connection Sharing settings.

To change global session values, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Global - Sessions** subcategory.
3. In the **Video Session Timeout** area, select or clear the **Enabled** check box. If you enable the video session time-out, specify the time-out value in the **Minutes** list. This value indicates the number of minutes the appliance will wait to close an inactive video session. You can select a value from the list or enter a value in the range of 1 to 60 minutes.
4. In the **Video session preemption timeout** area, select or clear the **Enabled** check box. If you enable the preemption warning, specify the time-out value in the **Seconds** list. This value indicates the number of seconds the appliance will wait for a user to respond to a preemption warning. You can select a value from the list or enter a value in the range of 5 to 120 seconds.
5. In the **Encryption Levels** area, select one or more levels of encryption to encode keyboard and mouse data sent over a video session to the appliance. The highest level enabled is used. Repeat this step for the Video encryption level.

   Video encryption is optional, but at least one Keyboard/Mouse encryption level must be selected.

6. In the **Connection Sharing** area, select sharing options as needed. If you select **Enable Share Mode**, users can share KVM sessions for the same target device. If you select **Automatic Sharing,** secondary users can share KVM sessions without first requesting permission from the primary user. If you select **Exclusvie Connections**, primary users can designate a KVM session as exclusive (exclusive sessions cannot be shared). Selecting **Stealth Connections** enables administrators to monitor a target device undetected. You can also specify in the **Input Control Timeout** field the number of seconds the appliance will wait for activity before transferring keyboard and mouse control from the primary user to the secondary user.
7. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

Configuring Global Virtual Media settings

Use the **Global - Virtual Media** subcategory to specify the settings for Virtual Media sessions.

To change global session values, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Global - Virtual Media** subcategory.
3. In the **Session Control** area, select or clear the check boxes as needed. If you clear **Lock to KVM Session**, virtual media sessions can remain after the Video Session that starts it closes. If you select **Allow Reserved Sessions**, then the owner of the virtual media session can choose to prevent other users from establishing a KVM session to the same target device. Also when the virtual media session is reserved, the corresponding KVM session is not subject to inactivity time-outs and cannot be preempted. If you select **Read-Only Access**, write access to Virtual Media sessions is prevented.
4. In the **Encryption Levels** area, select zero or more levels of encryption to encode Virtual Media data sent over a video session to the appliance. The highest level enabled is used.
5. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

Configuring Global Authentication settings

There are two types of user accounts: internal and external. Internal (local) user accounts reside within the appliance itself, while external user accounts are stored on an external authentication server. The **Users** category provides methods for managing internal user accounts.

The **Global - Authentication** category specifies the type and order of any authentication methods used. If a method fails or is unavailable, the software uses the next enabled authentication method.

Local authentication is always available as the primary or backup authentication method, and cannot be disabled.

See “Licensing appliance options” on page 87 for information on enabling LDAP.

To change authentication settings, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Global - Authentication** subcategory.
3. To specify an authentication method, select the check box next to the method in the **Authentication Settings** area.
4. When you specify more than one authentication method, you can control the order in which they are tried by changing the order in the list. Select a method and then click one of the **Reorder Authentication Methods** buttons. Click the **up** button to shift the selected method up; click the **down** button to shift the selected method down.
5. You can choose to use LDAP for authentication only, not for authorization, when using the local user database for authorization. Select or clear the check box next to **Use LDAP for Authentication Only** as needed.
6. You can choose to validate the values entered by the user for LDAP-related fields in either the **Search Parameters** or **Query Parameters** tab. Select or clear the check box next to **LDAP Syntax Validation** as needed.
7. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

For example, if LDAP is enabled as the first authentication method, followed by Local, the following process occurs:

- The appliance attempts LDAP authentication by querying its Management Information Base (MIB) to obtain the LDAP parameters specified in the **LDAP Parameters** field, which are then sent to and verified on the LDAP directory service.
- If LDAP authentication fails, the appliance attempts local authentication.
- If local authentication also fails, an error code is returned for the highest priority authentication method attempted, which in this case is LDAP.

6.3 Configuring LDAP

LDAP is a vendor-independent protocol standard used for accessing, querying, and updating a directory using TCP/IP. Based on the X.500 Directory Services model, LDAP is a global directory structure that supports strong security features including authentication, privacy, and integrity.

LDAP authentication configuration parameters

If individual user accounts are stored on an LDAP-enabled directory service, such as Active Directory, you can use the directory service to authenticate users.

The default values given for the LDAP search and query parameters are defined for use with Active Directory.

The settings made in the **Global - Authentication** subcategory of the AMP **Settings** tab let you configure your authentication configuration parameters. The software sends the ServSelect IP Software user name, password, and other information to the appliance, which then determines whether the ServSelect IP Software user has permission to view or change configuration parameters for the appliance in the AMP.

Important: Unless otherwise specified, the LDAP default values should be used unless Active Directory has been reconfigured. Modifying the default values may cause LDAP authentication server communication errors.

LDAP server parameters

Clicking the **Server Parameters** tab displays the parameters that define LDAP server connection information.

The **IP Address** fields specify the host names or IP addresses of the primary and secondary LDAP servers. These values cannot be loopback addresses or all zeros.

The second LDAP server is optional.

The **Port ID** fields specify the User Datagram Protocol (UDP) port numbers that are used to communicate with the LDAP servers. The default value is 389 for non-secure LDAP and 636 for secure LDAP. The default Port ID is automatically entered by the software when an access type is specified.

The **Access Type** radio buttons specify how a query is sent to each LDAP target device. Click **LDAP** to send a query as clear text (non-secure LDAP) or **LDAPS** to send a query using a Secure Socket Layer (SSL) (secure LDAP).

NOTE: When using **LDAP**, all user names, passwords, etc. sent between an appliance and LDAP server are sent as non-secure, clear text. Use **LDAPS** for secure, encrypted communication between an appliance and LDAP server.

LDAP search parameters

Clicking the **Search Parameters** tab displays the parameters used when searching for LDAP directory service users.

Use the **Search DN** field to define an administrator-level user that the KV2116, KV4116, or ServSelect III VM uses to log into the directory service. Once the appliance is authenticated, the directory service grants it access to the directory to perform the user authentication queries specified on the **Query Parameters** tab. The default values are *cn=Administrator*, *cn=Users*, *dc=yourDomainName*, and *dc=com* and may be modified. For example, to define an administrator Distinguished Name (DN) for test.view.com, type *cn=Administrator*, *cn=Users*, *dc=test*, *dc=view*, and *dc=com*. This is a required field unless the directory service has been configured to enable anonymous search, which is not the default.

Each **Search DN** value must be separated by a comma. The **Search Password** field is used to authenticate the administrator or user specified in the **Search DN** field.

Use the **Search Base** field to define a starting point from which LDAP searches begin. The default values are *dc=yourDomainName*, *dc=com*, and may be modified. For example, to define a search base for test.com, type *dc=test*, *dc=com*. Each **Search Base** value must be separated by a comma.

The **UID Mask** field specifies the search criteria for User ID searches of LDAP target devices. The format should be in the form *<name>=<%1>*. The default value is *sAMAccountName=%1*, which is correct for use with Active Directory. This field is required for LDAP searches.

LDAP Query Parameters

Clicking the **Query Parameters** tab displays the parameters used when performing user authentication queries.

The appliance performs two different types of queries. Query mode (appliance) is used to authenticate administrators attempting to access the appliance itself. Query mode (device) is used to authenticate users that are attempting to access attached target devices.

Additionally, each type of query has three modes that utilize certain types of information to determine whether or not a ServSelect IP Software user has access to an appliance or connected target devices.

You can configure the following settings in the **Query Parameters** tab:

- The **Query Mode (Appliance)** parameters determine whether or not a ServSelect IP Software user has access to the appliance.
- The **Query Mode (Device)** parameters determine whether or not a ServSelect IP Software user has user access to target devices connected to an appliance. The user does not have access to the appliance.
- The **Group Container**, **Group Container Mask**, and **Target Mask** fields are only used for group query modes and are required when performing an appliance or device query.
- The **Group Container** field specifies the organizational unit (ou) created in Active Directory by the administrator as the location for group objects. Group objects are Active Directory objects that can contain users, computers, contacts, and other groups. **Group Container** is used when **Query Mode** is set to Group. Each group object, in turn, is assigned members to associate with a particular access level for member objects (people, appliances, and target devices). The access level associated with a group is configured by setting the value of an attribute in the group object. For example, if the **Notes** property in the group object is used to implement the access control attribute, the **Access Control Attribute** field in the **Query Parameters** tab should be set to *info*. Setting the **Notes** property to **KVM User Admin** causes the members of that group to have user administration access to the appliances and target devices that are also members of that same group.

  The **Notes** property is used to implement the access control attribute. The value of the **Notes** property, available in group and user objects shown in Active Directory Users and Computers (ADUC), is stored internally in the directory, in the value of the *info* attribute. ADUC is a Microsoft Management Console snap-in for configuring Active Directory. It is started by selecting **Start > Programs > Administrative Tools > Active Directory Users and Computers**. This tool is used to create, configure and delete objects such as users, computers and groups. See Figure 6-2 on page 76 and Figure 6-3 on page 77 for more information.
- The **Group Container Mask** field defines the object type of the **Group Container**, which is normally an organizational unit. The default value is “ou=%1”.
- The **Target Mask** field defines a search filter for the target device. The default value is “cn=%1”.
- The **Access Control Attribute** field specifies the name of the attribute that are used when the query modes are set to Attribute. The default value is *info*.

Appliance and target device query modes

One of three different modes can each be used for **Query Mode (Appliance)** and **Query Mode (Device)**:

- **Basic** – A user name and password query for the ServSelect IP Software user is made to the directory service. If they are verified, the ServSelect IP Software user is given

administrator access to the appliance and any attached target devices for **Query Mode (Appliance)**, or to any selected target device for **Query Mode (Device)**.

- **Attribute** – A user name, password, and **Access Control Attribute** query for the appliance user is made to the directory service. The **Access Control Attribute** is read from the user object (the user account) in Active Directory.

  If the value "KVM Appliance Admin" is found, the ServSelect IP Software user is given appliance administrator access to the appliance and any attached target devices for **Query Mode (Appliance)**, or to any selected target device for **Query Mode (Device)**. If the value "KVM User Admin" is found, the ServSelect IP Software user is given User administrator access to the appliance and attached target devices for **Query Mode (Appliance)**, or to any selected target device for **Query Mode (Device)**.

  The following are examples showing how the **KVM Appliance Admin** and **KVM User Admin** attribute modes are defined in Active Directory for a user named John Smith, stored in the ADUC. You can access the ADUC by selecting **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

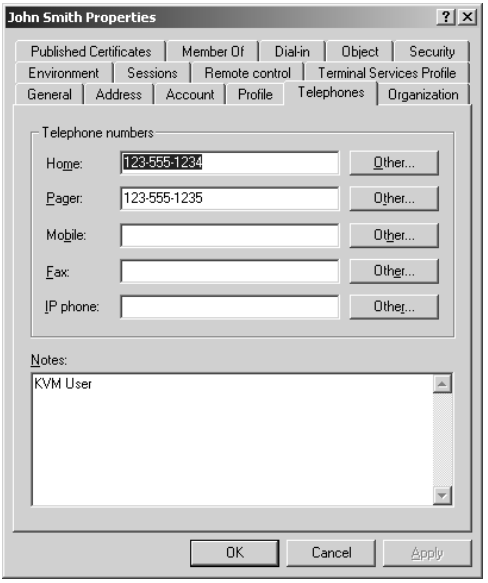

Figure 6-2. Active Directory - KVM user

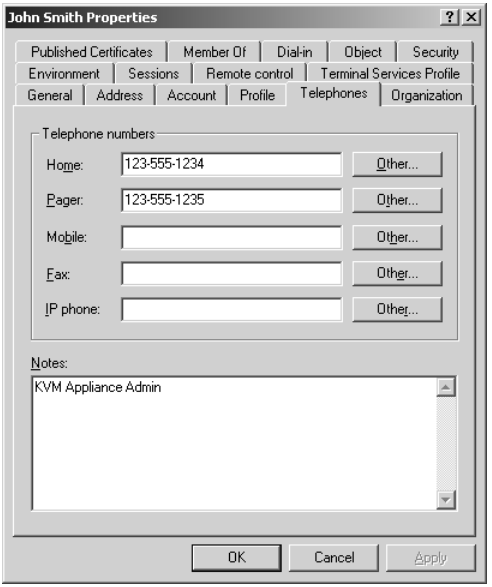

Figure 6-3. Active Directory - KVM appliance admin

- **Group –** A user name, password, and group query is made to the directory service for an appliance and attached target devices when using **Query Mode (Appliance)**, or for a selected target device when using **Query Mode (Device)**. If a group is found containing the user and the appliance name, the ServSelect IP Software user is given access to the appliance or attached target devices, depending on the group contents, when using **Query Mode (Appliance)**. If a group is found containing the user and target device IDs, the ServSelect IP Software user is given access to the selected target device connected to the appliance when using **Query Mode (Device)**.

  Groups can be nested to a maximum of 16 levels in depth. Use nesting to create groups within other groups. For example, you may have a top-level group named Computers that contains a member named R&D, which is a group. The R&D group may contain a member named Domestic, which is a group, and so on.

  The following is an example of groups defined in Active Directory.

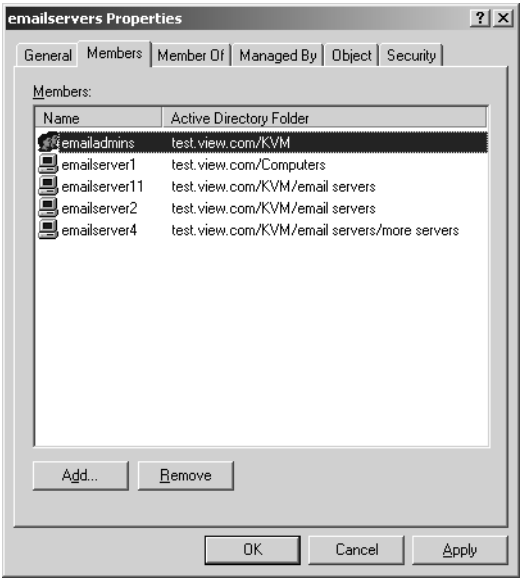

Figure 6-4. Active Directory - Define groups

Setting up Active Directory for performing queries

Before you can use any of the querying modes for units, you must first make changes to Active Directory so that the selected querying mode can assign the applicable authorization level for the ServSelect IP Software user.

To set up group queries, complete the following steps:

1. Log into Windows with administrator privileges.
2. Open Active Directory software.
3. Create an organizational unit to be used as a group container.
4. Create an object in Active Directory with a name identical to the switching system name for querying appliances (specified in the **Name** field in the **SNMP** category of the AMP), or identical to the attached target devices for querying target devices (specified in the **Devices** category of the AMP). The name must match exactly, including case.

   The appliance names and target device names used for group queries are stored in the appliance. The appliance name and target device names specified in the **SNMP** and **Devices** categories of the AMP must identically match the object names in Active Directory. Each appliance name and target device name may be comprised of any combination of upper-case and lower-case letters (a-z, A-Z), digits (0-9) and hyphens (-). You cannot use spaces and periods (.) or create a name that consists entirely of digits. These are Active Directory constraints. The factory default ServSelect III VM name in earlier versions contains a space that must be removed by editing the switching system name in the **SNMP** category of the AMP.
5. Create one or more groups under the group container organizational unit.

6. Add the user names and target device and appliance objects to the groups you created in step 5.
7. Specify the value of any attribute being used to implement the access control attribute. For example, if you are using *info* as the attribute in the **Access Control Attribute** field and using the **Notes** property in the group object to implement the access control attribute, the value of the **Notes** attribute in Active Directory may be set to one of the three available access levels (**KVM User**, **KVM User Admin**, or **KVM Appliance Admin**) for the group object. The members of the group may then access the appliances and target devices at the specified access level.

6.4 Managing local user accounts

The **Users** category lists user names in the appliance user database and their access levels. You can add, modify, or delete a user account from this category. The security lock-out feature is also controlled from this category.

The fields in this category are disabled if LDAP is being used for both Authentication and Authorization. If LDAP is being used only for Authentication, then users can be added and modified in this category, but only to set the access control lists for the users (the password fields are disabled in this mode).

Assigning user rights

You can assign users one of three access levels: user, user administrator, or appliance administrator. Use the user access level to assign individual target device access rights to a user.

Access levels

The following table indicates the types of appliance operations that can be performed in the three access levels.

KV2116, KV4116, or ServSelect III VM appliance access levels

Operations	Appliance administrator	User administrator	User
Preempt other users	All	Equal and lesser	No
Set network and global values	Yes	No	No
Reboot and upgrade firmware	Yes	No	No
Manage user accounts	Yes	Yes	No
Monitor target device status	Yes	Yes	No
Access target devices	Yes	Yes	Assigned by Admin

To add or modify a user, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Users** category.
3. Complete one of the following steps:
   - To add a new user, click the **Add** button. The Add User window opens.

- To modify a user, select a user name and click the **Modify** button. The Modify User window opens.

4. Complete one of the following steps:
   - When adding a user, enter the user name and password to assign to the user and then verify the password by typing it in the **Verify Password** field.
   - When modifying a user, change the password, if needed.

   When **Use LDAP for Authentication only** is selected in the **Global - Authentication** category, the password field is disabled and only the access rights of the user are used.
5. Select the needed access level for this user from the pull-down menu. If you select the **User** option, the **Access Rights** button is visible.
   a. To select individual target device access for the user, click the **Access Rights** button. The User Access Rights window opens.
   b. To add access to target devices, select one or more target devices in the left (No access to) column. Click the **Add** button.
   c. To remove access to target devices, select one or more target devices in the right (Allow access to) column. Click the **Remove** button.
   d. Repeat steps b and c until the right (Allow access to) column represents the applicable target device access for this user, and then click **OK**.
6. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

To delete a user, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Users** category.
3. Select the user or users to delete.
4. Click the **Delete** button. You are prompted to confirm the deletion.
5. Click **Yes** to confirm the deletion.
6. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

NOTE:
Add, Modify and Delete user operations may be combined and saved at the same time by pressing the **Apply** or **OK** buttons on the AMP when done with the changes.

Locking and unlocking user accounts

When the security lock-out feature is enabled, and a user enters an invalid password five consecutive times, that user account is disabled for a specified number of hours, or until it is unlocked or the appliance is rebooted. If a locked-out user tries to log in during the lock-out period, an error message is displayed. A closed-lock icon is visible next to the names of locked-out users on the AMP **Users** category. Security lock-out, when enabled, applies to all local user accounts on the appliance, but not to LDAP users.

An appliance administrator can specify the lock-out period. A user administrator can unlock only user accounts; an appliance administrator can unlock any type of account.

When the security lock-out feature is disabled, no users are locked-out. Disabling security lock-out has no effect on users who are already locked-out.

To enable or disable security lock-out, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **User**s category.
3. Complete one of the following steps:
   - Select the **Enable Lock-outs** check box. Enter the number of hours (1 to 99) in the lock-out period in the **Duration** field.
   - Clear the **Enable Lock-outs** check box.
4. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

To unlock an account, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **User**s category.
3. Select the user to unlock.
4. Click the **Unlock** button.
5. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

A locked-out user is unlocked if the appliance is rebooted or when the configured lock-out duration expires.

6.5 Managing user sessions

The **Status** tab displays information about currently active Video Viewer and virtual media sessions. Each line of session information includes:

- The status of the session. A Locked icon is shown for KVM sessions that are locked to virtual media sessions, and a Reserved icon is shown for reserved virtual media sessions.
- The name of the user who is logged in to the session.
- The length of time this session has been active, in the form hours:minutes:seconds. If the session has been active for more than 24 hours, the number of days precedes the other time information. For example, a session that has been active for two days, three hours, seven minutes, and 52 seconds shows 2d 3:07:52.
- The type of session, including both virtual media sessions and KVM sessions. The session status also displays the video session type, such as KVM (Stealth). For more information on session types see Table 4.1.
- The name of the target device to which this session is connected. If the session is connected to a SAM cable with no target device name specified in the database, the

SAM cable eID is listed. If the session is connected to a cascade switch, the SAM cable eID, appliance name, and channel number are listed.

- The IP address of the remote client connected to this session.

To disconnect a user session, complete the following steps:

1. Click the **Status** tab in the AMP.
2. Select one or more users sessions to disconnect. Use the Shift or Ctrl key to select multiple user sessions.
3. Click the **Disconnect Session** button. A message prompts you to confirm the disconnect request.
4. Complete one of the following steps:
   - Click **Yes** to disconnect the user sessions.
   - Click **No** to cancel the disconnect.
5. Click *Apply* to save any changes without exiting the AMP.
   - or -
   Click *OK* to save any changes and exit the AMP.
   - or -
   Click *Cancel* to exit the AMP without saving any changes.

6.6 Viewing and changing Server Access Module settings

The **Server Access Modules** category displays information about each SAM cable, including its input port number, ID, type, language, and status. The possible status values are:

- Green circle = the SAM cable is online
- Yellow circle = the SAM cable is upgrading
- Red X = the SAM cable is offline

To display SAM cable information, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Server Access Modules** category.

To remove offline conversion options from the list, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Server Access Modules** category.
3. Click **Clear Offline**.

To change the language reported by USB SAM cables, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Server Access Modules** category.
3. Click **Language**.
4. Select the keyboard layout from the list.
5. Complete one of the following steps:

- Click **OK** to select the keyboard layout.
- Click **Cancel** to return to the AMP without changing the language.

6. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

All Server Access Modules report in the new language.

If you have previously used the Resync Wizard to retrieve offline SAM information to store in the local database, and later use the Clear Offline in the ServSelect IP Software, you should resynchronize again to remove them from the local database. For more information, see Resynchronizing the ServSelect IP Database Server Listing topic.

The clear offline feature cannot clear offline SAM adaptors displayed on the local port OSD of a tiered appliance.

6.7 Using SNMP

The **SNMP** category specifies general SNMP configuration information. The **SNMP - Traps** subcategory indicates which traps are enabled and disabled.

SNMP (Simple Network Management Protocol) is a protocol used to communicate management information between network management applications and appliances. SNMP managers (such as Tivoli and HP OpenView) can communicate with the appliance by accessing MIB-II (Management Information Base) and the public portion of the enterprise MIB. MIB-II is a standard MIB that many SNMP managers support. You can:

- Enable or disable SNMP operations.
- Enter switching system information and community strings.
- Indicate which computers can manage the appliance. If you enter one or more allowable managers, only those IP addresses can monitor the appliance using SNMP. If you do not enter any allowable managers, then the appliance can be monitored using SNMP from any IP address.
- Indicate which computers receive SNMP traps from the appliance. If you do not specify any trap destinations, no traps are sent.

When you enable SNMP, the unit responds to SNMP requests over UDP port 161. Port 161 is the standard UDP port used to send and receive SNMP messages.

The AMP uses SNMP within a secure tunnel to manage appliances. For this reason, UDP port 161 does not need to be exposed on firewalls. You must expose UDP port 161 to monitor appliances using third party SNMP-based management software.

Configuring general SNMP settings

To configure general SNMP settings, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **SNMP** category.
3. Select or clear the **Enable SNMP** check box.
4. In the **Name** field, enter the 0 to 255 character fully qualified domain name of the appliance. In the **Contact** field, enter 0 to 255 characters of contact information.
5. In the **Community Names** area, enter the 1 to 64 character **Read**, **Write**, and **Trap** community names. These specify the community strings that must be used in SNMP

actions. The **Read** and **Write** strings apply only to SNMP over UDP port 161 and act as passwords that protect access to the appliance.

6. In the **Allowable Managers** area, specify up to four SNMP management entities to monitor the appliance, or leave this area blank to let any computer to monitor the appliance.

   To add an allowable manager, complete the following steps:

   a. Click the **Add** button. The Allowable Manager window opens.
   b. Enter the IP address of the management computer.
   c. Click **OK** to add the management computer.

   To modify an allowable manager, complete the following steps:

   a. Select an entry in the **Allowable Managers** list, then click the **Modify** button. The Allowable Manager window opens.
   b. Modify the entry as needed.
   c. Click **OK** to save the change.

   To delete an allowable manager, complete the following steps:

   a. Select one or more entries in the **Allowable Mangers** list, then click the **Delete** button. You are prompted to confirm the deletion.
   b. Click **Yes** to confirm the deletion.

7. In the **Trap Destinations** area, specify up to four destinations to which this appliance sends traps.

   To add a trap destination, complete the following steps:

   a. Click the **Add** button. The Trap Destination window opens.
   b. Enter the IP address of the trap destination.
   c. Click **OK** to add the trap destination.

   To modify a trap destination, complete the following steps:

   a. Select one or more entries in the **Trap Destinations** list, then click the **Modify** button. The Trap Destination window opens.
   b. Modify the entry as needed.
   c. Click **OK** to save the change.

   To delete a trap destination, complete the following steps:

   a. Select an entry in the **Trap Destinations** list, then click the **Delete** button. You are prompted to confirm the deletion.
   b. Click **Yes** to confirm the deletion.

8. Complete one of the following steps:

   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

9. If you clicked **Apply** or **OK**, you are prompted to confirm a reboot. The new settings are not used until the appliance reboots. Complete one of the following steps:

   - Click **Yes** to reboot the appliance. The AMP displays the status and indicates when the reboot is complete.
   - Click **No** to reboot at a later time.

Managing SNMP traps

An SNMP trap is a notification sent by the appliance to a management computer, indicating that an event has occurred in the appliance that can require further attention. You can specify which individual SNMP traps are sent to the management computers by selecting the corresponding check boxes, or you can enable or disable all traps. The KV2116, KV4116, and ServSelect III VM appliance have enterprise traps. To interpret these traps correctly, download the corresponding trap MIB from the Black Box Web site.

To enable or disable SNMP traps, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **SNMP - Traps** subcategory. A list of traps is displayed. Traps that are currently enabled are selected; disabled traps are not selected.
3. Complete one of the following steps:
   - Select or clear the individual trap check boxes.
   - To enable all traps, click the **Enable All** button.
   - To disable all traps, click the **Disable All** button.
4. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

6.8 Viewing target device connection information

The **Devices** category displays connection information for each target device, as follows:

- **SAM** - The display shows the eID of the SAM cable.
- **Cascaded switch** - The display shows the appliance and all of its channels.
- **No device connection** - The display indicates “None”.

When you select the **Devices** category for the first time, the AMP retrieves the target devices that exist in the software database as well as information on how the target devices are connected to the selected appliance. The Connections column lists the current target device connection. This can be to either a SAM cable or a cascade switch. If connected to a SAM cable, the SAM cable eID is visible in the Connections column. If connected to a cascade switch, the cascade switch and all of its channels are visible. If no unit is currently connected to the path, then this field displays “None”.

Clicking on a hyperlink of a target device entry opens the Video Viewer.

You can resynchronize the database on the computer with the database on the appliance from this category.

Modifying target device names

The **Devices** category can be used to modify the target device name on both the appliance and in the client database.

To modify the name of a target device, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Devices** category.

3. Select the target device from the list that you want to modify. You can only modify one target device at a time.
4. Click **Modify**.
5. The pop-up window lists the current name of the target device as stored in both the appliance and the client database (not necessarily the same).
6. Type the new name of the target device in the **New Name** field.
7. Complete one of the following steps:
   - Click **OK** to change the target device name.
   - Click **Cancel** to keep the target device name as is.
8. Repeat the steps 3 through 7 for each target device name that you want to change.
9. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

Resynchronizing the target device list

You might need to resynchronize the target device list if the local user has changed target device names on the appliance using the OSD interface or if SAM cables have been added or moved. For more information about names, see "Target device naming" on page 7.

Prior to starting the resynchronization process, a warning message indicates that the database will be updated to match the current configuration in the appliance. This warning contains a check box that indicates whether offline SAM cables will be included. When enabled, target devices associated with SAM cables that are offline are included. When disabled, offline SAM cables are not included and any existing target devices associated with them in the database are removed.

This procedure only resynchronizes your own ServSelect IP Software client. To keep databases consistent when you have multiple computers using the software, save your resynchronized local database and restore it to the other computers.

To resynchronize the target device list, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Devices** category.
3. Click the **Resync** button. The Resync Wizard opens. Click **Next**.
4. A warning message indicates that the database will be updated to match the current configuration in the appliance. Select or clear the **Include Offline Server Access Modules** check box. Click **Next**.
5. A Polling Appliance message is displayed with a progress bar indicating that appliance information is being retrieved.
6. Complete one of the following steps:
   - If no changes were detected in the appliance, a completion window opens with this information. Click **OK**.
   - If target device changes were detected, the Detected Changes window opens. Click **Next** to update the database.
   - If a cascade switch was detected, the Enter Cascaded Switch Information window opens. Select the type of cascade switch connected to the appliance from

the pull-down menu. If the type you are looking for is not available, you can add it using the **Add** button. For more information, see "Configuring cascade switch connections" on page 87. Click **Next**.

7. The completion window opens. Click **Finish** to exit.

6.9 Configuring cascade switch connections

The **Cascade Switches** category displays tiered cascade switch information, including the SAM cable eIDs, cascade switch type, and the port to which each is connected.

Setting a connection

To configure a cascade switch connection, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Cascaded Switches** category.
3. Complete one of the following steps:
   - Click the pull-down list next to the cascade switch and select the cascade switch type to assign.
   - If the cascade switch type is not in the pull-down list, add a cascade switch to the **Existing Cascaded Switches** list by clicking the **Add** button. The Add Cascaded Switch window opens.

     Type the name of the cascade switch and select the cascade switch type from the list.

     Click **OK** to add the cascade switch. The cascade switch is now in the **Existing Cascaded Switches** list and in the Cascade Switch pull-down list.
4. Repeat step 3 for each cascade switch to be configured.
5. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

6.10 Viewing versions

Version information

The **Versions** category displays firmware version numbers.

SAM cable version information

The **Versions - SAMs** subcategory displays SAM cable version information. You can individually view and upgrade SAM cables from this category.

Hardware version information

The **Versions - Hardware** subcategory displays the hardware component version numbers of the unit.

6.11 Licensing appliance options

When you click the **Licensed Options** category in the AMP, the Licensed Options window opens. Use this window to configure options for use that are available on the KV2116, KV4116, or ServSelect III VM firmware. The Licensed Options window lists

each option available on the KV2116, KV4116, or ServSelect III VM and if the option has been enabled by a license key.

To license a KV2116, KV4116, or ServSelect III VM option, complete the following steps:

1. Click the **Licensed Options** category in the left column in the AMP.
2. Click the **Add** button on the right side of the window to add a KV2116, KV4116, or ServSelect III VM option. The Enter Key window opens.
3. Type a license key. The license key is comprised of 20 case-sensitive characters.
4. Click **OK**. If the key for the option you are licensing is valid, the license type is listed in the Option Name column and Yes is listed in the Options Enabled column for the licensed option.

NOTE:
Currently, the only available option is **LDAP Authentication**.

6.12 Upgrading firmware

You can upgrade the firmware for either the KV2116, KV4116, or ServSelect III VM appliance or the SAM cables.

Automatic SAM cable firmware upgrades

You can set the AMP to upgrade the SAM cable firmware automatically.

To enable automatic SAM cable firmware upgrades, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Select the **Versions - SAMs** subcategory.
3. Enable the check box next to **Enable Auto-Upgrade for all Server Access Modules**.
4. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

Upgrading KV2116, KV4116, or ServSelect III VM appliance firmware

To upgrade appliance firmware, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Upgrade Appliance Firmware** button.

   If you have made changes in the Settings tab of the AMP but have not yet applied them, a warning message prompts you to confirm the upgrade. The firmware upgrade requires an appliance reboot and pending changes will be discarded.

   To apply changes to the Settings tab before the upgrade, complete the following steps:

   a. Click **No** to cancel the appliance firmware upgrade.

   b. Click **Apply**.

c. Continue with step 2 of this procedure, or click **Yes** to discard pending (unapplied) changes.

3. The Firmware Upgrade window opens. You can choose to use TFTP or ASMP file transfer. When upgrading a ServSelect III VM appliance, only the TFTP option is available.
   To use TFP, complete the following steps:
   a. Select the **TFTP Server** radio button.
   b. In the **TFTP Server IP Address** field, type in the IP address of the TFTP target device where the firmware is installed.
   c. In the **Firmware Filename** field, enter the name of the firmware file.
   d. Click the **Upgrade** button. The AMP tracks and displays status.
4. To use ASMP, complete the following steps:
   a. Select the **File System** radio button.
   b. Click **Browse** to select the firmware file to be transferred.
   c. Click the **Upgrade** button. The AMP tracks and displays status.
5. When the upgrade is complete, a message prompts you to confirm a reboot. Complete one of the following steps:
   - Click **Yes** to reboot the appliance. After rebooting, the AMP re-establishes a secure management connection with the appliance.
   - Click **No** to reboot at a later time. You must reboot to use the new firmware.
6. Click **Close** to exit the Firmware Upgrade window.

Important: Do not turn off the KV2116 or KV4116 appliance while it is upgrading.

Upgrading SAM cable firmware

SAM cables can be upgraded individually or simultaneously as a group by SAM cable type. When an upgrade is started, the current status is listed.

When you request an upgrade for all SAM cables of a particular type, that upgrade must finish before you can start another upgrade for any SAM cable of that type. However, multiple individual SAM cable firmware upgrades can be done in parallel.

To simultaneously upgrade the firmware of multiple SAM cables, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Upgrade SAM Firmware** button. The Upgrade SAM Firmware window opens.
3. Select the check box in front of each type of SAM cable to upgrade. (A check box for a SAM cable type can only be selected if there is a later version available of the firmware. This is indicated by the Need Upgrade column. If one or more SAM cables of a given type need upgrades, you can select this type for the upgrade. If there is no later firmware for a SAM cable type, you cannot select the corresponding check box.)
4. Click **Upgrade**. The Status column displays either In Progress, Succeeded, or Failed (with reason included) depending on the status of each SAM cable upgrade. A Firmware upgrade currently in progress message is visible until all of the selected SAM cable types are upgraded.
5. When complete, a message prompts you to confirm the upgrade completion. When confirmed, the **Upgrade** button is again enabled.

6. Click **Close** to exit the Upgrade SAM Firmware window.

To upgrade SAM cable firmware individually, complete the following steps:

1. Click the **Settings** tab in the AMP.
2. Click the **Versions - Server Access Modules** subcategory.
3. To view firmware information, select the SAM cable from the eID pull-down menu list. Each entry is a combination of the port number, the eID, and either the target device name or cascade switch name, depending on what is attached to the SAM cable. If the SAM cable is not attached to anything, the menu displays **None**. When a SAM cable is selected, its firmware information is listed in the **Information** field.
4. Compare the current information to the **Firmware Available** field to see the firmware upgrade available for the SAM cable. (You can load firmware even if the current and available versions are the same. In some cases, you can downgrade the SAM cable to an earlier, compatible version.) Click the **Load Firmware** button.
5. The firmware upgrade begins. During the upgrade, progress messages are visible below the **Firmware Available** field. When the upgrade is finished, a message indicates either that the upgrade is complete or the reason for failure.
6. Repeat steps 3 through 5 for each SAM cable to upgrade.
7. When finished, click **OK**.

6.13 Rebooting the appliance

The Reboot Appliance tool instructs the appliance to reboot. The appliance broadcasts a disconnect message to all client connections before rebooting.

To reboot the appliance, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Reboot Appliance** button. A message prompts you to confirm the reboot. Click **Yes** to confirm the request. The appliance notifies each attached client, then reboots.
3. The AMP closes.

6.14 Managing the appliance configuration database

All appliance settings are stored in an appliance configuration database. (User account information is stored in a user database; see “Managing the appliance user database” on page 91 for more information.)

Saving an appliance configuration database

The Save Appliance Configuration tool saves the configuration database from the appliance to a file on the computer running the software.

The file is encrypted during the save process, and you are prompted to create a password when you save the database. You must enter this password when you restore the file.

To save a configuration from an appliance to a file, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Save Appliance Configuration** button. The Save Appliance Configuration window opens.

3. Click **Browse** and navigate to a location to save the configuration file. The location is listed in the **Save To** field.
4. Click **Save**. The Enter Password window opens.
5. Enter a password in the **Password** field, then repeat the password in the **Verify Password** field. This password is requested when you restore this database to an appliance. Click **OK**.
6. The appliance configuration database file is read from the appliance and saved to the selected location. Progress messages are visible. When the save is complete, you are prompted to confirm the completion. Click **OK** to return to the Tools tab.

Restoring an appliance configuration database

The Restore Appliance Configuration tool restores a previously-saved configuration database from the computer running the software to the appliance. The database file can be restored to either the appliance from which it was saved or to another appliance of the same type. This eliminates the need to manually configure a new appliance.

To restore a configuration file to an appliance, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Restore Appliance Configuration** button. The Restore Appliance Configuration File window opens.
3. Click **Browse** and navigate to the location where you stored the saved configuration file. The filename and location are listed in the **File Name** field.
4. Click **Restore**. The Enter Password window opens.
5. Enter the password you created when the configuration database was saved. Click **OK**.
6. The configuration file is written to the appliance. Progress messages open. You are prompted to confirm a reboot. The restored configuration file is not used until the appliance reboots. Complete one of the following steps:
   - Click **Yes** to reboot the appliance. The AMP displays the status and indicate when the reboot is complete.
   - Click **No** to reboot at a later time.

6.15 Managing the appliance user database

All user accounts and access rights assignments are stored in a database.

The file is encrypted during the save process, and you are prompted to create a password when you save the database. You must enter this password when you restore the file.

Saving an appliance user database

The Save Appliance User Database tool saves this user database from the appliance to a file on the computer running the software.

To save a user database from an appliance to a file, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Save Appliance User Database** button. The Save Appliance User Database window opens.

3. Click **Browse** and navigate to a location to save the user database file. The location is listed in the **Save To** field.
4. Click **Save**. The Enter Password window opens.
5. Enter a password in the **Password** field, then repeat the password in the **Verify Password** field. This password is requested when you restore this database to an appliance. Click **OK**.
6. The user database file is read from the appliance and saved to a location. Progress messages open. When the save is complete, you are prompted to confirm the completion. Click **OK** to return to the Tools tab.

Restoring an appliance user database

The Restore Appliance User Database tool restores a previously-saved user configuration database from the computer running the software to the appliance. The database file can be restored to either the appliance from which it was saved or to another appliance of the same type. This eliminates the need to manually configure users on a new appliance.

To restore a user database file to an appliance, complete the following steps:

1. Click the **Tools** tab in the AMP.
2. Click the **Restore Appliance User Database** button. The Restore Appliance User Database window opens.
3. Click **Browse** and navigate to the location where you stored the saved user database file. The filename and location is listed in the **File Name** field.
4. Click **Restore**. The Enter Password window opens.
5. Enter the password you created when the user database was saved. Click **OK.**
6. The user database file is written to the appliance. Progress messages open. When complete, the new user database is used immediately; no reboot is required.

Enabling NFS Support

Port data can be logged to a networked file system for ease of distribution.

To enable NFS Support at a Global level:

1. Click the Settings Tab in the AMP.
2. Select the Global – NFS subcategory.
3. Click the box labeled Enable NFS.
4. In the areas provided, enter the configuration information appropriate to your file system.
5. Complete one of the following steps:
6. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

To enable NFS Support for a specific port:

1. Click the Settings Tab in the AMP.
2. Select the Ports – NFS subcategory.

3. Click the box labeled Enable NFS.
4. In the areas provided, enter the configuration information appropriate to your file system.
5. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

Specifying a Network Time Protocol Server

To ensure that all network devices are synchronized, the ServSelect IP software may be configured to reference a NTP server on a regular basis.

To enable NTP Support:

1. Click the Settings Tab in the AMP.
2. Select the Global – NTP subcategory.
3. Click the box labeled Enable NTP.
4. You may enter the IP address for up to two NTP servers in the blanks provided. Once entered, their status will be displayed to the right of their IP address.
5. In the field labeled Update, enter the time between updates in hours.
6. Complete one of the following steps:
   - Click **Apply** to save any changes without exiting the AMP.
   - Click **OK** to save any changes and exit the AMP.
   - Click **Cancel** to exit the AMP without saving any changes.

Appendix A: About the SCPS AMP

After you add an SCPS appliance to ServSelect IP Software, you may view and configure unit parameters, view and control active Telnet server sessions and execute a variety of control functions. These operations are accomplished through the SCPS Appliance Management Panel (AMP).

The SCPS AMP has three tabs: Settings, Status and Tools, as follows:

- •The Settings panel contains categories in the left portion of the panel. Categories with a preceding plus sign (+) have subcategories. The content of the remaining area of the panel changes according to the category or subcategory that is selected.
- Settings categories include general appliance information, Command Line Interpreter (CLI) configuration data, user accounts, port configuration data, SNMP and other appliance and server configuration information.
- •The Status panel displays information about currently active Telnet server sessions.
- •The Tools panel allows you to execute control functions on the appliance such as rebooting, saving/restoring databases and upgrading firmware.

Some operations that you initiate through the SCPS AMP will trigger a dialog box indicating that a reboot is required in order for the change to take effect. In such cases, you may choose to reboot immediately or wait to reboot later.

For more information about the appliance and its operations, see the ServSelect IP SCPS Installer/User Guide.

To access the AMP:

1. Click the *Appliances* tab in the ServSelect IP Software Explorer.
2. Double-click on an SCPS appliance in the Unit list.
   -or-
   Select an SCPS appliance from the Unit list, then click the *Manage Appliance* task button.
   -or-
   Right-click on an SCPS appliance in the Unit list. Select *Manage Appliance* from the pop-up menu.
   -or-
   Select an SCPS appliance in the Unit list and press **Enter**.
3. A password prompt appears. Type your username and password and click *OK*. The default username is **Admin** with no password.

NOTE:
ServSelect IP Software caches your user credentials until the application is closed. You do not need to re-enter your credentials for each session.

4. The SCPS AMP appears.

To exit the AMP:

Click *OK* to save any changes and exit the AMP.
-or-
Click *Cancel* to exit the AMP without saving any changes.

Viewing Global Settings

The Global category displays the appliance's product type and serial number (EID). This information cannot be modified.

Configuring Global Network Settings

The Global - Network subcategory specifies the appliance's IP address, subnet mask, gateway and MAC address (read-only).

To change global network values:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Global - Network* subcategory.
3. In the IP Address field, enter the appliance's address in IP dot notation. The value cannot be a loopback address or all zeros.
4. In the Subnet Mask field, enter the appliance's subnet mask in IP address dot notation. The value cannot be a loopback address or all zeros.
5. In the Gateway field, enter the appliance's gateway address in IP address dot notation. The value cannot be a loopback address. If there is no gateway address, enter **Ø.Ø.Ø.Ø**.
6. Click *pply* to save any changes without exiting the AMP.
   -or-
   Click *K* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

Configuring Global CLI Settings

The Global - CLI subcategory specifies the CLI port, terminal type and whether users may connect to other ports from the CLI port. This subcategory also specifies the following:

- Modem initialization - If this field contains a non-zero value, the SCPS assumes a modem is attached to the serial CLI port. At bootup and each time the SCPS detects modem power up, this string is sent to the modem to initialize it for call reception. Modem power up is detected by a transition of DSR from low to high.
- Connect control - When this feature is enabled, a user may connect to other serial ports from the CLI port. When disabled, connecting to another serial port from the CLI port is not allowed.
- CLI access character - During a Telnet session to a server, when a user enters this character while simultaneously pressing the **Control** key, the CLI mode is accessed.
- PP settings - When PPP is enabled, you specify the local IP address that will be used to communicate with this SCPS over a PPP connection on the serial CLI port. You also specify the remote IP address for the client that connects to the SCPS over the PPP connection. A subnet mask may also be included.

To change CLI settings:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Global - CLI* subcategory.
3. In the Port field, select the port identifier from the pulldown menu. If you do not wish to assign a port for the CLI, select *CLI not Assigned* from the menu.

4. In the Terminal Type field, select the terminal emulation type for the CLI port from the pulldown menu.
5. In the Modem Initialization field, enter a 0-64 character string containing the command to set the modem to autoanswer mode.
6. In the Connect Control field, select *Enabled*or *Disabled* from the pulldown menu to indicate whether a user may connect to other serial ports from the CLI port.
7. In the CLI Access Character field, enter a caret (^) and the character that will be used to access CLI mode during a server session. The character entered after the caret may be a letter or one of the following: left bracket ([), right bracket (]), caret (^), underscore (_) or backslash (\).
8. In the PPP Settings area, enable or disable the Enabled checkbox.
9. In the Local IP Address field, enter the address to be used to communicate with this SCPS, in IP dot notation. The value cannot be a loopback address or all zeros.
10. In the Remote IP Address field, enter the address of the client that will connect to this SCPS, in IP dot notation. The value cannot be a loopback address or all zeros.
11. In the Subnet Mask field, enter the subnet mask for the PPP connection, in IP dot notation. The value cannot be a loopback address or all zeros.
12. Click *Apply* to save any changes without exiting the AMP.
    -or-
    Click *OK* to save any changes and exit the AMP.
    -or-
    Click *Cancel* to exit the AMP without saving any changes.

Configuring Global Authentication Settings

The Global - Authentication subcategory specifies the type and order of the authentication methods that will be used. If RADIUS authentication will be used, the RADIUS server information is also specified in this panel.

Changing global authentication settings

To change authentication settings:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Global - Authentication* subcategory.
3. To disable all authentication methods, enable the *No Authentication* checkbox. You cannot disable all authentication if SSH is enabled; in this case, you should disable SSH in the Global - Sessions subcategory, then disable all authentication in the Global - Authentications subcategory.
4. To specify one or more authentication methods, enable one or more checkboxes next to the method.
5. When you specify more than one authentication method, you may change their order in the list. Select a method and then click one of the Reorder Authentication Methods buttons. Click the *up* button to shift the selected method up; click the *down* button to shift the selected method down.
6. The RADIUS Servers area is valid only if RADIUS is one of the enabled authentication methods. If RADIUS is enabled, the following information must be set for the primary server; information for the secondary server is optional.

a. In the IP Address fields, enter the addresses of the RADIUS servers in IP dot notation. These values cannot be loopback addresses or all zeros.

b. In the Shared Secret field, enter the 8-24 character strings that will be used to communicate with the RADIUS servers. These values must also be configured on the RADIUS servers; see the RADIUS system administrator or documentation for server-specific configuration information.

c. In the Access Rights Id. fields, enter the attributes that identify the access rights stored on the RADIUS servers for this appliance. These values must also be configured on the RADIUS servers; see the RADIUS system administrator or documentation for server-specific configuration information.

d. In the UDP Port fields, enter the UDP port numbers that will be used to communicate with the RADIUS servers, in the range 1-65535.

e. In the Time-Out fields, enter the number of seconds to wait for a reply from the RADIUS servers, in the range 1-60.

f. In the Retry Count fields, enter the number of attempts that will be made to authenticate a user after a time-out on the RADIUS servers, in the range 1-10.

7. Click *Apply* to save any changes without exiting the AMP.
   -or-
   Click *OK* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

Configuring Global Session Settings

The Global - Sessions subcategory specifies:

- How history buffer data is handled at the start and end of the Telnet session. You may have the data sent to the virtual terminal window automatically when a Telnet session is established (Auto) or have it held until it is explicitly requested (Hold). You may also retain the history buffer content when the Telnet session ends (Keep) or discard it (Clear).
- Whether the appliance will automatically close an inactive Telnet session. When enabled, the Telnet session is closed when the SCPS does not receive any data within a specified number of minutes.
- Whether the appliance will allow plain text sessions.
- SSH settings, including the ability to enable and disable SSH, specify or modify an SSH authentication mode, create an SSH key and display the current SSH fingerprints.

Either plain text sessions or SSH (or both) must be enabled in order to launch Serial Console Viewer Telnet sessions. Failure to have either or both enabled will result in an invalid configuration. Plain text sessions are enabled by default.

To specify history buffer control:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Global - Sessions* subcategory.
3. In the History Buffer Control area, select *Auto* or *Hold* for the Session Start action. Select *Keep* or *Clear* for the Session End action.
4. Click *Apply* to save any changes without exiting the AMP.
   -or-

Click *OK* to save any changes and exit the AMP.
-or-
Click *Cancel* to exit the AMP without saving any changes.

To specify session time-out settings:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Global - Sessions* subcategory.
3. Enable or disable the *Enabled* checkbox in the Serial session timeout area. If time-out is disabled, a session will not time-out.
4. If session time-out is enabled, specify the time-out value. You may choose a value from the Minutes pulldown menu or you may enter a value in the range 1-90 minutes.
5. Click *Apply* to save any changes without exiting the AMP.
   -or-
   Click *OK* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

To enable or disable plain text sessions:

NOTE:
Either plain text sessions or SSH (or both) must be enabled.

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Global - Sessions* subcategory.
3. Enable or disable the *Allow Plain text Sessions* checkbox.
4. Click *Apply* to save any changes without exiting the AMP.
   -or-
   Click *OK* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

Viewing and configuring SSH information

The SSH Settings area of the Settings - Session subcategory lists the current SSH configuration and status information, as follows:

- SSH Status may be Enabled, Disabled, In Progress or Failed.
- Host Key Status may be either Key Exists or No Key.
- SSH Authentication Mode indicates what will be used to authenticate users: a password, a key, a password or a key (in either order) or a password and a key (in either order). The mode is configured when SSH is enabled or modified.

A user's SSH key is created and modified in the Users category.

To view and configure SSH settings:

NOTE:
Either plain text sessions or SSH (or both) must be enabled.

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Global - Sessions* subcategory.
3. To enable SSH:

a. Click the *Enable SSH* button. The Enable SSH dialog box appears.
b. Select the SSH Authentication Mode from the pulldown menu.
c. If no SSH key exists, the Create new key checkbox will automatically be checked (that is, a new key will be created); you cannot disable it.
d. If an SSH key exists and you wish to create a new key, enable the *Create new key* checkbox.
   -or-
   To use the existing key, disable the *Create new key* checkbox.
e. Click *OK* to close the dialog box. SSH is now enabled.

To change the SSH authentication mode:

a. Click the *Modify SSH* button. The Modify SSH dialog box appears.
b. Select the SSH authentication mode from the pulldown menu, then click *OK* to close the dialog box. Any changes will now take effect.

To disable SSH:

a. Click the *Disable SSH* button. A confirmation dialog box appears.
b. To delete the SSH key, enable the *Delete Key* checkbox.
   -or-
   To retain the SSH key, disable the *Delete Key* checkbox.
c. Click *OK* to confirm the deletion and close the dialog box.
   SSH is now disabled.

To view key information, click the *Fingerprints* button. The SSH Fingerprints dialog box will display the MD5 hash and bubble babble. Click *OK* to close the dialog box.

Managing User Accounts

The Users category lists usernames and their access levels. You may add, modify or delete a user account from this dialog box. Up to 64 user accounts may be created. The Security Lock-out feature is also controlled from this panel.

A user may be assigned one of three access levels: user, user administrator or appliance administrator. The user access level allows you to assign individual server access rights to a user.

The following table indicates the types of appliance operations that may be performed in each access level

Table A.1: Appliance operations

Operations	Appliance Administrator	User Administrator	User
Preemption	All	Equal and Lesser	Equal and Lesser
Configure and global settings	Yes	No	No
Reboot	Yes	No	No

Table A.1: Appliance operations

Operations	Appliance Administrator	User Administrator	User
Upgrade FLASH	Yes	No	No
Mange user accounts	Yes	Yes	No
Configure port settings	Yes	No	No
Monitor server status	Yes	Yes	No
Issue break signal	Yes	Yes	Yes
Access server(s)	Yes	Yes	Assigned by Admin

Locking and unlocking user accounts

When the Security Lock-out feature is enabled, and a user enters an invalid assword five consecutive times, that user's account will be disabled for a specified number of hours, or until it is expressly unlocked or the appliance is power-cycled. If a locked-out user tries to log in during the lock-out period, an error message is displayed. A closed-lock icon appears next to the names of locked-out users. Security Lock-out, when enabled, applies to all user accounts.

An appliance administrator may specify the lockout period. A user administrator may unlock only user accounts; an appliance administrator may unlock any type of account.

When the Security Lock-out feature is disabled, no users will be locked-out.

NOTE:
Disabling Security Lock-out has no effect on users who are already locked-out.

Adding or modifying a user

To add or modify a user:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Users* category.
3. To add a new user, click the *Add* button. The Add User dialog box appears.
   -or-
   To modify a user, select the name and then click the *Modify* button. The Modify User dialog box appears.
4. When adding a user, enter the 3-16 character username in the Name field. Spaces are not allowed.
5. Enter a 3-16 character password in the Password field. Spaces are not allowed. Verify the password by typing it again in the Verify Password field.
6. Select the appropriate access level from the pulldown menu. If you select *User*, the Access Rights button appears.
   a. To select individual server access for the user, click the *Access Rights* button. The User Access Rights dialog box appears.

b. To add access to a server, select a server in the left (No access to) column. Click the *Add* button.

c. To remove access to a server, select a server in the right (Allow access to) column. Click the *Remove* button.

d. Repeat steps b and c until the right (Allow access to) column represents the appropriate server access for this user, and then click *OK*.

7. To configure a user's public SSH key:

   a. Enter a 1-1024 character key in the Key Text field.
   -or-
   Click the *Browse* button to navigate to the path/filename containing an SSH key. The public key contained in the selected file will appear in the Key Text field.
   -or-
   Click the *Create* button.

   b. The Create SSH Key Pair dialog box appears. The Identity File field contains the private key filename and path. You may click the *Browse* button to specify a path and filename for the public/private key files to change the Identity File field content. By default, these key files are stored under <install_dir>\"userkeys".

   c. Enter a secret pass phrase for accessing the private key file in the Pass Phrase field. Asterisks will be displayed instead of the actual data you enter. If you leave this field blank, your key will not be encrypted.

   d. Repeat the pass phrase in the Pass Phrase Again field.

   e. You may optionally place information in the Comments field.

   f. Click the *Generate* button. The text area of the dialog box displays help information and senses movement as the mouse is dragged across it. Move the mouse to assist the random number generator; it passes a seed that is based on the mouse's location. A progress bar indicates the completion percentage.

   g. When the completion percentage reaches 100, the dialog box closes, a confirmation dialog box is displayed and the generated key will appear in the Key Text field of the Add User or Modify User dialog box.

8. Click *OK* to save the settings and return to the Users panel.

9. Click *Apply* to save any changes without exiting the AMP.
   -or-
   Click *OK* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

NOTE:
Each user must have a password to be able to access the SCPS AMP. This requirement is independent of any configured SSH authentication mode that may use the password.

To delete a user:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Users* category.
3. Select the user(s) to delete.
4. Click the *Delete* button. You are prompted to confirm the deletion.

5. Click *Yes* to confirm the deletion.
   -or-
   Click *No* to cancel the deletion.
6. Click *Apply* to save any changes without exiting the AMP.
   -or-
   Click *OK* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

To enable or disable Security Lock-out:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *User*s category.
3. Enable the *Enable Lock-outs* checkbox. Enter the number of hours (1-99) in the lock-out period in the Duration field.
   -or-
   Disable the E*nable Lock-outs* checkbox. The Duration field is disabled.
4. Click *Apply* to save any changes without exiting the AMP.
   -or-
   Click *OK* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

To unlock an account:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *User*s category.
3. Select the user to unlock.
4. Click the *nlock* button. The lock icon next to the username will disappear.
5. Click *Apply* to save the change without exiting the AMP. The user will be able to attempt to log in again.
   -or-
   Click *OK* to save the change and exit the AMP. The user will be able to attempt to log in again.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

A locked-out user will also be unlocked if the appliance is power-cycled or when the configured lock-out duration expires.

Managing User Sessions

The Status tab displays information about currently active Telnet sessions. Each line of session information includes:

- The name of the user who is logged in to the session.
- The length of time this session has been active, in the form hours:minutes:seconds. If the session has been active for more than 24 hours, the number of days precedes the other time information. For example, a session that has been active for two days, three hours, seven minutes and 52 seconds will show 2d 3:07:52.
- The name of the server to which this session is connected.
- The IP address of the connected client.

To disconnect a user session:

1. Click the *Status* tab in the SCPS AMP.
2. Select one or more sessions to disconnect. Press the **Shift** key to select multiple sessions.
3. Click the *Disconnect Session* button. A message prompts you to confirm the disconnect request.
4. Click *Yes* to disconnect the user(s).
   -or-
   Click *No* to cancel the disconnect.

Configuring Serial Port Parameters

The Ports category lists all configuration parameters for the 8 or 16 ports on the SCPS. You may change any port parameter except the name and type.

Modifying a port

To modify a port:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Port*s category.
3. Select a port and click the *odify* button. The Modify Port dialog box appears.
4. To change the session time-out, enter a value in the Session Timeout field in the range 1-90.
   -or-
   Choose a value from the pulldown menu. If you choose *Global Setting*, the value specified in Global - Sessions will be used.
5. To change the CLI access character, enter a caret (^) and a character in the CLI Access Character field. The character entered after the caret may be a letter or one of the following: left bracket ([), right bracket (]), caret (^), underscore (_) or backslash (\). To change the CLI access character, enter a single character in the CLI Access Character field.
   -or-
   Choose a value from the pulldown menu. If you choose *Global Setting*, the value specified in Global - CLI will be used.
6. To change the Telnet port number, enter a value in the range 3000-65000 in the Telnet Port Number field.
7. To change the baud rate, choose a value from the pulldown menu in the Baud Rate field.
8. To change the number of data bits, choose a value from the pulldown menu in the Data Bits field.
9. To change the parity, choose a value from the pulldown menu in the Parity field.
10. To change the number of stop bits, choose a value from the pulldown menu in the Stop Bits field.
11. To change the flow control method, choose a value from the pulldown menu in the Flow Control field. This value cannot share the same signal as the Power On Signal value.
12. To change the toggle signal, choose a value from the pulldown menu in the Toggle Signal field.

13. To change the power on signal, choose a value from the pulldown menu in the Power On Signal field. This value cannot share the same signal as the Flow Control value.
14. Click *OK* to save the changes locally and exit the dialog box. If any field is invalid, an error message will appear and the focus will be set to the field in error.
    -or-
    Click *Cancel* to exit the dialog box without saving changes locally.
15. Click *Apply* to save any changes to the SCPS without exiting the AMP.
    -or-
    Click *OK* to save any changes to the SCPS and exit the AMP.
    -or-
    Click *Cancel* to exit the AMP without saving any changes.

Configuring Port Alert Strings

The Ports - Alerts subcategory lists the defined alert strings for a specified port. You may create, modify or delete alert strings for each port. Each port may have up to ten alert strings.

To create, modify or delete port alert strings:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Ports - Alerts* subcategory.
3. Select a port/server from the Server pulldown menu. The Alert Strings list will contain the alert strings that have already been defined for that server. If fewer than ten alert strings have been defined, the list will also contain a <*new*> entry.
4. To create an alert string:
    a. Select <*new*> in the Alert Strings list.
    b. In the text box under the list, enter 3-32 characters.
    c. When complete, click the *Check Mark* button.

To modify an alert string:

a. Select the string in the Alert Strings list. The selected string will appear in the text box under the list.
b. Modify the alert string in the text box.
c. When complete, click the *Check Mark* button next to the text box.

To delete an alert string:

a. Select the string in the Alert Strings list.
b. Click the *X* button below the list.

To copy all the alert strings defined for one port to another port or to all other ports:

a. In the Server pulldown menu, select the port from which to copy the alert strings. That port's alert strings will be listed.
b. From the Copy To pulldown menu, select the port to which the alert strings will be copied.
    -or-
    Select *All*, which will copy the alert string to all ports on this SCPS.
c. lick the *Copy* button. You are prompted to confirm the copy operation.

d. Click *Yes* to confirm the copy.
-or-
Click *No* to cancel the copy.

5. Click *Apply* to save any changes without exiting the AMP.
-or-
Click *OK* to save any changes and exit the AMP.
-or-
Click *Cancel* to exit the AMP without saving any changes.

Viewing Port Statistics

The Ports - Statistics subcategory displays SCPS port statistics and EIA signal settings, as follows:

- The Port and Name columns contain the port's number and name.
- The Tx Bytes and Rx Bytes columns indicate the number of bytes transmitted and received.
- The Errors column indicates the number of errors.
- The Power Status column indicates the port's power status.
  The possible values are:

  On = Power on *On = Power on and value toggled since last poll

  Off = Power off *Off = Power off and value toggled since last poll
- The remaining columns contain strings that represent a portion of the port's EIA signals:

  TD = Transmit Data DSR = Data Set Ready

  RD = Receive Data DCD = Data Carrier Detect

  RTS = Request to Send RI = Ring Indicator

  CTS = Clear to Send SIG3 = SIG3

  DTR = Data Terminal Ready SIG4 = SIG4

The possible values in each of these columns are:

On = Power on *On = Power on and value toggled since last poll

Off = Power off *Off = Power off and value toggled since last poll

To display port statistics:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Ports - Statistics* subcategory.

Managing SNMP

The SNMP category specifies general SNMP configuration information. The SNMP - Traps subcategory indicates which traps are enabled and disabled.

SNMP (Simple Network Management Protocol) is a protocol used to communicate management information between network management applications and appliances. Other SNMP managers (such as Tivoli and HP OpenView) may communicate with your appliance by accessing MIB-II (Management Information Base) and the public portion of the enterprise MIB. MIB-II is a standard MIB that many SNMP servers support. You may:

- Enable or disable SNMP operations.

- Enter system information and community strings.
- Indicate which stations may manage the appliance. If you enter one or more allowable managers, only those IP addresses will be able to manage the appliance via SNMP. If you do not enter any allowable managers, the appliance may be managed via SNMP from any IP address.
- Indicate which stations (destinations) will receive SNMP traps from the appliance. If you do not specify any trap destinations, no traps will be sent.

When you enable SNMP, the unit will respond to SNMP requests over UDP (User Datagram Protocol) port 161. Port 161 is the standard UDP port used to send and receive SNMP messages.

NOTE:
The SCPS AMP uses SNMP within a secure tunnel to manage appliances. For this reason, UDP port 161 need not be exposed on firewalls. You will need to expose UDP port 161 to monitor Black Box appliances via third party SNMP-based management software.

Managing SNMP traps

An SNMP trap is a notification sent by the appliance to a management station, indicating that an event has occurred in the appliance that may require further attention. You may specify which individual SNMP traps are sent to the management stations by simply enabling the appropriate checkboxes, or you may enable/disable all traps. The SCPS has enterprise traps.

To configure general SNMP settings:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *SNMP* category.
3. Enable or disable the *Enable SNMP* checkbox.
4. In the Name field, enter the system's 0-255 character fully qualified domain name. In the Contact field, enter 0-255 characters of contact information.
5. In the Community Names area, enter the 1-64 character Read, Write and Trap community names. These specify the community strings that must be used in SNMP actions. The Read and Write strings only apply to SNMP over UDP port 161 and act as passwords that protect access to the appliance.
6. In the Allowable Managers area, specify up to four SNMP management entities to monitor this appliance, or leave this area blank to allow any station to monitor the appliance.

Adding an Allowable Manager

To add an Allowable Manager:

a. Click the *Add* button. The Allowable Manager dialog box appears.
b. Enter the IP address of the management station.
c. Click *OK* to add the management station.

To modify an Allowable Manager:

a. Select an entry in the Allowable Managers list, then click the *Modify* button. The Allowable Manager dialog box appears.
b. b.Modify the entry as needed.
c. c.Click *OK* to save the change.

To delete an Allowable Manager:

a. Select an entry in the Allowable Mangers list, then click the *Delete* button. You will be prompted to confirm the deletion.

b. Click *Yes* to confirm the deletion.

Trap destinations

7. In the Trap Destinations area, specify up to four SNMP trap destinations to which this appliance will send traps.

To add a trap destination:

a. Click the *Add* button. The Trap Destination dialog box appears.

b. Enter the IP address of the trap destination.

c. Click *OK* to add the trap destination.

To modify a trap destination:

a. Select an entry in the Trap Destinations list, then click the *Modify* button. The Trap Destination dialog box appears.

b. Modify the entry as needed.

c. Click *OK* to save the change.

To delete a trap destination:

a. Select an entry in the Trap Destinations list, then click the *Delete* button. Youwill be prompted to confirm the deletion.

b. Click *Yes* to confirm the deletion.

8. Click *Apply* to save any changes without exiting the AMP.
   -or-
   Click *OK* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

To enable or disable SNMP traps:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *SNMP - Traps* subcategory. A list of traps is displayed. Traps that are currently enabled are checked; disabled traps are unchecked.
3. Enable or disable the individual traps' checkboxes.
   -or-
   To enable all traps, click the *Enable All* button.
   -or-
   To disable all traps, click the *Disable All* button.
4. Click *Apply* to save any changes without exiting the AMP.
   -or-
   Click *OK* to save any changes and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

Viewing Server Connection Information

The Servers category displays connection information for each server. The Connections column identifies the port to which the server is connected. If there is no server connection, the Servers column will indicate *None*.

Clicking on a connection launches the Serial Console Viewer.

You may resynchronize the database on your system with the database on the appliance from this panel.

Resynchronizing the server list

During the resynchronization process, a warning message will indicate that the database will be updated to match the current configuration in the appliance. This warning contains a checkbox that indicates whether servers that are configured with default names should be excluded. If servers are excluded, they will not be added to (or they may be removed from) the database if they already exist in the database. Excluded servers will only be removed from the database if there are no other connections to the server.

NOTE:
This procedure only resynchronizes your own ServSelect IP Software client. To ensure consistency when you have multiple systems using ServSelect IP Software, save your resynchronized local database and restore it to the other systems.

To resynchronize the server list:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Servers* category.
3. Click the *Resync* button. The Resync Wizard launches. Click *Next*.
4. A warning message will indicate that the database will be updated to match the current configuration in the appliance. Enable or disable the *Exclude Servers with Default Names* checkbox. Click *Next*.
5. A Polling Appliance message box is displayed with a progress bar indicating that appliance information is being retrieved.
6. If no changes were detected in the appliance, a completion window appears with this information.
   -or-
   If server changes were detected, the Detected Changes window will be displayed. Click *Next* to update the database.
7. The completion window appears. Click *Finish* to exit.

Upgrading Firmware

You may display the current firmware revision numbers for an SCPS. You may also upgrade the SCPS firmware. When an upgrade is initiated, the current status will be displayed. While an upgrade is in progress, you cannot initiate another.

To view the appliance firmware revision numbers:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Versions* category.

To upgrade appliance firmware:

1. Click the *Tools* tab in the SCPS AMP.
2. Click the *Upgrade Appliance Firmware* button.

If you have made changes in the Settings panel of the AMP but have not yet applied them, a warning message prompts you to confirm the upgrade. The process requires an appliance reboot and pending changes will be discarded.

To apply changes to the Settings panel before the upgrade:

a. Click *No* to cancel the appliance firmware upgrade.
b. Click *Apply*.
c. Continue with step 2 of this procedure.

-or-

To discard pending (unapplied) changes, click *Yes*.

3. The Firmware Upgrade dialog box appears. From the Firmware Type pulldown menu, select the type of firmware to be upgraded.
4. In the TFTP Server IP Address field, enter the IP address of the TFTP server where the firmware is located, in IP dot notation. This field initially contains the value retrieved from the SCPS, which you may modify. The value cannot be a loopback address or all zeros.
5. In the Firmware Filename field, enter the path/filename of the firmware file. This field initially contains the value retrieved from the SCPS.
6. Click the *Upgrade* button. Progress messages will appear.
7. When the upgrade is complete, a message prompts you to confirm a eboot. Click *Yes* to eboot the appliance. The Upgrade irmware dialog box will display progress information and will indicate when the reboot is complete.
   -or-
   lick *No* to reboot at a later time. You must reboot to use the new firmware.
8. Click *Close* to exit the Firmware Upgrade dialog box.

Rebooting the Appliance

When the Reboot Appliance tool is selected, the SCPS broadcasts a disconnect message to any active users, then logs out the current user and reboots.

To reboot the appliance:

1. Click the *Tools* tab in the SCPS AMP.
2. Click the *Reboot* button. A message prompts you to confirm the reboot. Click *Yes* to confirm the request. The appliance will reboot.

Managing Appliance Configuration Databases

All appliance settings are stored in an appliance configuration database. (User account information is stored in a user database; see *Managing User Databases* in this chapter for more information.)

The Save Appliance Configuration tool saves the appliance database from the appliance to a file on the system running ServSelect IP Software.

The Restore Appliance Configuration tool restores a previously-saved appliance configuration database from the system running ServSelect IP Software to the appliance. The database file may be restored to either the appliance from which it was saved or to another appliance of the same type. This eliminates the need to manually configure a new appliance.

NOTE:
The file is encrypted during the save process, and you will be prompted to create a password when you save the database. You will need to enter this password when you restore the file.

Saving a configuration file

To save a configuration from an appliance to a file:

1. Click the *Tools* tab in the SCPS AMP.
2. Click the *Save Appliance Configuration* button. The Save Appliance Configuration dialog box appears.
3. Click *Browse* and navigate to a location to save the configuration file. The location appears in the Save To field.
4. Click *Save*. The Enter Password dialog box appears.
5. Enter a password in the Password field, then repeat the password in the Verify Password field. This password will be requested when you restore this database to an appliance. Click *OK*.
6. The appliance configuration database file is read from the appliance and saved to a location. Progress messages are displayed. When the save is complete, a confirmation message is displayed. Click *OK* to return to the Tools panel.

To restore a configuration file to an appliance:

1. Click the *Tools* tab in the SCPS AMP.
2. Click the *Restore Appliance Configuration* button. The Restore Appliance Configuration File dialog box appears.
3. Click *Browse* nd navigate to the location where you stored the saved configuration file. The filename and location appears in the File name field.
4. Click *Restore*. The Enter Password dialog box appears.
5. Enter the password you created when the configuration database was saved, then re-enter the password in the Verify Password field. Click *OK*.
6. The configuration file is written to the appliance. Progress messages are displayed. When the restore is complete, a confirmation message is displayed. Click *OK* to return to the Tools panel.

Managing Appliance User Databases

All user accounts and access rights assignments are stored in a database. (Configuration information is stored in a configuration database; see *Managing Appliance Configuration Databases* in this chapter for more information.)

The Save Appliance User Database tool saves this user database from the appliance to a file on the system running ServSelect IP Software.

The Restore Appliance User Database tool restores a previously-saved user configuration database from the system running ServSelect IP Software to the appliance. The database file may be restored to either the appliance from which it was saved or to another appliance of the same type. This eliminates the need to manually configure users on a new appliance.

NOTE:
The file is encrypted during the save process, and you will be prompted to create a password when you save the database. You will need to enter this password when you restore the file.

Saving a user database

To save a user database from an appliance to a file:

1. Click the *Tools* tab in the SCPS AMP.
2. Click the *Save Appliance User Database* button. The Save Appliance User Database dialog box appears.
3. Click *Browse* and navigate to a location to save the user database file. The location appears in the Save To field.
4. Click *Save*. The Enter Password dialog box appears.
5. Enter a password in the Password field, then repeat the password in the Verify Password field. This password will be requested when you restore this database to an appliance. Click *OK*.
6. The user database file is read from the appliance and saved to a location. Progress messages are displayed. When the save is complete, a confirmation message is displayed. Click *OK* to return to the Tools panel.

Viewing and Changing SCPS Port Settings

The Settings - Ports category of the SCPS AMP lists all configuration parameters for the 8 or 16 ports on the SCPS. You may change any port parameter except the name and type.

To modify a port:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Ports* category.
3. Change or view the port information.
4. Click *OK* to save the changes locally and exit the dialog box. If any field is invalid, an error message will appear and the focus will be set to the field in error.
   - or -
   Click *Cancel* to exit the dialog box without saving changes locally.
5. Click *Apply* to save any changes to the SCPS without exiting the AMP.
   - or -
   Click *OK* to save any changes to the SCPS and exit the AMP.
   -or-
   Click *Cancel* to exit the AMP without saving any changes.

Choosing an Encryption Method for SCPS Appliances

When launching a Serial Console Viewer session to an SCPS server, ServSelect IP Software may use either an SSH or plain text (non-encrypted) session, depending on the settings of the SCPS appliance connected to the server. The SCPS appliance can be set to support SSH sessions only, plain text sessions only, or both types of sessions at the same time.

When the appliance is set to support both types of sessions, the Encryption Method dialog box is displayed. You may then use the dialog box to choose whether or not to use SSH and to save your choice for future Serial Console Viewer sessions.

You can choose to enable SSH Serial Console Viewer connections to SCPS servers, or to use no encryption. When an SSH connection is initiated, the Serial Console Viewer is launched on top of an SSH tunnel. SSH settings are configured in the SCPS AMP.

To Choose an Encryption Method:

1. Click the **Servers** tab in the ServSelect IP Software Explorer.
2. Double-click on the SCPS server in the Unit list.
   -or-
   Select the SCPS server, then click the **Connect Serial** task button.
   -or-
   Right-click on the SCPS server. Select **Connect Serial** from the pop-up menu.
   -or-
   Select the SCPS server and press **Enter**.
3. If the SCPS is configured to allow either an SSH or plain text (no encryption) connection, the Encryption Method dialog box displays.
4. Click **Keep choice as default setting** to indicate that the selection you make be maintained for subsequent launch requests during the current ServSelect IP Software session.
   -or-
   Continue to step 5 to display the Encryption Method dialog box each time the Serial Console Viewer is launched.
5. Click **Yes** to launch the Serial Console Viewer using an SSH tunnel.
   -or-
   Click **No** to launch the Serial Console Viewer using no encryption.
6. The Serial Console Viewer displays.

NOTE:
The Encryption Choice dialog box will not reappear during the current ServSelect IP Software session, unless a Clear Login Credentials is performed.

Adding, Modifying and Deleting Trap Destinations on SCPS Appliances

Add up to four SNMP trap destinations to which this appliance will send traps in the Trap Destination area. You may also modify and delete existing SNMP Trap Destinations

To add a trap destination:

1. Click the *Add* button. The Trap Destination dialog box appears.
2. Enter the IP address of the trap destination.
3. Click *OK* to add the trap destination.

To modify a trap destination:

1. Select an entry in the Trap Destinations list, then click the *Modify* button. The Trap Destination dialog box appears.
2. Modify the entry as needed.
3. Click *OK* to save the change.

To delete a trap destination:

1. Select an entry in the Trap Destinations list, then click the *Delete* button. You will be prompted to confirm the deletion.
2. Click *Yes* to confirm the deleti

Viewing the SCPS Firmware Version

You can display the current firmware revision numbers for an SCPS.

To view the SCPS appliance firmware revision numbers:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Versions* category.

Configuring the Public SSH Key on SCPS Appliances

To configure a user's public SSH key:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Users* category.
3. Click *Add/Modify* to add a new user.
   - or -
   Select a user in the list and click *Modify.*
4. In the SSH Public Key area, enter a 1-1024 character key in the Key Text field.
   - or -
   Click the *Browse* button to navigate to the path/filename containing an SSH key. The key contained in the selected file will appear in the Key Text field.
   - or -
   Click the *Create* button.
5. The SSH2 Key Pair Generator dialog box appears. The Identity File field contains the private key filename and path. You may click the Browse button to specify a path and filename for the public/private key files to change the Identity File field content. By default, these key files are stored under <install_dir>\"userkeys".
6. Enter a secret pass phrase for accessing the private key file in the Pass Phrase field. Asterisks will be displayed instead of the actual data you enter. If you leave this field blank, your key will not be encrypted.
7. Repeat the pass phrase in the Pass Phrase Again field.
8. You may optionally place information in the Comments field.
9. Click the *Generate* button. The Key Pair Random Number Generator dialog box appears. The text area of this dialog box displays help information and senses movement as the mouse is dragged across it. Move the mouse to assist the random number generator; it passes a seed that is based on the mouse's location. A progress bar indicates the completion percentage.
10. When the completion percentage reaches 100, click the *Close* button (clicking this button before the completion percentage reaches 100 will cancel the key generation process). The dialog box will close and the generated key will appear in the Key Text field of the Add User or Modify User dialog box.
11. Click *OK* to save the settings and return to the Users panel.
12. Click *Apply* to save any changes without exiting the AMP.
    - or -
    Click *OK* to save any changes and exit the AMP.
    -or-
    Click *Cancel* to exit the AMP without saving any changes.

Setting User Access Rights for SCPS Appliances

A user can be assigned one of three access levels: user, user administrator or appliance administrator. The user access level allows you to assign individual server access rights to a user.

To set user access rights:

1. Click the *Settings* tab in the SCPS AMP.
2. Select the *Users* category.
3. Select the appropriate access level from the pulldown menu. If you select *User*, the Access Rights button appears.
    a. To select individual server access for the user, click the *Access Rights* button. The User Access Rights dialog box appears.
    b. To add access to a server, select a server in the left (No access to) column. Click the *Add* button.
    c. To remove access to a server, select a server in the right (Allow access to) column. Click the *Remove* button.
    d. Repeat steps b and c until the right (Allow access to) column represents the appropriate server access for this user, and then click *OK*.

Adding, Modifying and Deleting Allowable Managers on SCPS Appliances

Add up to four SNMP management entities to monitor this appliance or leave this blank to allow any station to monitor the appliance in the Allowable Managers area. You may also modify or delete an existing allowable manager.

To add an Allowable Manager:

1. Click the *Add* button. The Allowable Manager dialog box appears.
2. Enter the IP address of the management station.
3. Click *OK* to add the management station.

To modify an Allowable Manager:

1. Select an entry in the Allowable Managers list, then click the *Modify* button. The Allowable Manager dialog box appears.
2. Modify the entry as needed.
3. Click *OK* to save the change.

To delete an Allowable Manager:

1. Select an entry in the Allowable Managers list, then click the *Delete* button. You will be prompted to confirm the deletion.
2. Click *Yes* to confirm the deletion.

Appendix B: Updating ServSelect IP Software

For optimal operation of the switching system, make sure that you have the latest version of ServSelect IP Software available from the Black Box Web site.

To update ServSelect IP Software, complete the following steps:

3. Go to http://www.blackbox.com and download the update file.
4. Double-click on the installer. The installer determines if a previous version of the software resides on the computer.
5. Complete one of the following steps:
   - If no previous version has been detected and a window opens to confirm the upgrade, click **Continue**.
   - If a previous version is detected and a window opens alerting you to another version of the product, click **Overwrite** to confirm the upgrade.
   - Click **Cancel** to exit without upgrading the software.
6. Installation starts. The Program Files, Shortcuts, Environment Variables, and the Registry Entries (for Windows operating systems), are installed or overwritten with the new files and settings of the current version.

Appendix C: Virtual media

Virtual media and USB 2.0 constraints

The virtual media feature of KV2116, KV4116, and ServSelect III VM appliances enables you to connect to the USB port of an attached computer. With this feature, a user located at the appliance or using the remote software can access a local USB storage device, such as a USB CD drive, diskette drive, or flash drive, from an attached computer.

The VM SAM USB2-VGA cable is a composite device that addresses four functions: keyboard, mouse, CD drive, and mass storage device. The CD drive and mass storage device will be present on the target device whether or not a virtual media session is mapped. If a media device is not mapped, it is shown without media present. When a virtual media device is mapped to the target device, the target device will be notified that media has been inserted. When the media device is unmapped, the target device will be notified that the media was removed. Therefore, the USB virtual device is not disconnected from the target device.

The VM SAM USB2-VGA cable presents the keyboard and mouse as a composite USB 2.0 device. Therefore the BIOS must support composite USB 2.0 human interface device (HID). If the BIOS of the connected computer does not support this type of device, the keyboard and mouse might not work until the operating system loads USB 2.0 device drivers. If this occurs, there might be a BIOS update provided by the computer manufacturer that will provide BIOS support for a USB 2.0 connected keyboard and mouse.

Booting a computer using virtual memory

In many cases the virtual media feature can boot an attached computer from a device attached to the USB port on the appliance. Most computers with a USB port can use virtual media; however, limitations in some USB media devices and the BIOS of some computers might prevent the computer from booting from a USB device attached to the KV2116, KV4116, or ServSelect III VM appliance.

Booting from a virtual USB device is dependant on the target device supporting booting from an external composite USB device. It also requires a CD of the operating system that supports external USB 2.0 booting. The following is a partial list of operating systems that support booting from an external USB 2.0 device:

- Windows Server 2003
- Windows XP
- Windows 2000 Server with Service Pack 4 (SP4) or later

To determine if your computer can be booted from virtual media, complete the following steps:

1. Connect a USB CD drive to the KV2116, KV4116, or ServSelect III VM appliance with an operating system installation CD that is bootable and map it to the target device. Reboot the target device to determine if it will boot from this attached CD drive. The BIOS might need to be set to boot from an external USB device.
2. If the target device will not boot, connect the USB CD drive to a USB port on the target device and reboot the target device. If the target device successfully boots from the CD drive, the BIOS is not supporting booting from a composite USB 2.0 device. Check the support Web site from the target device manufacturer to determine if a

later BIOS is available that might support booting from a composite USB 2.0 device. If so, update the BIOS and retry.

3. If the target device is not capable of booting from an external USB 2.0 device, try the following methods to remotely boot this target device:
   - Some BIOS versions provide an option to limit USB speeds. If this option is available to you, change the USB port setting to “USB 1.1” or “Full Speed” mode and try booting again.
   - Insert a USB 1.1 card and try booting again.
   - Insert a USB 1.1 Hub between the VM SAM USB2-VGA cable and the target device and try booting again.
   - Contact the manufacturer of the target device for information on availability or plans of a BIOS revision that will support booting from a composite USB 2.0 device.

Virtual media restrictions

The following list specifies restrictions for using virtual media:

- The KV2116, KV4116, or ServSelect III VM virtual media appliances only support connection of USB 2.0 diskette drives, flash drives, and CD drives.
- The ServSelect IP Software only supports mapping of USB 2.0 and USB 1.1 diskette drives and flash drives connected to the client computer.

Appendix D: Keyboard and mouse shortcuts

This appendix lists the keyboard and mouse shortcuts that can be used in Explorer.

Table D.1: Divider pane keyboard and mouse shortcuts

Operation	Description
F6	Navigates between the split-screens and gives focus to the last element that had focus.
F8	Gives focus to the divider.
Left or **Up Arrow**	Moves the divider left if the divider has the focus.
Right or **Down Arrow**	Moves the divider right if the divider has the focus.
Home	Gives the right pane of the split-screen all of the area (left pane is hidden) if the divider has the focus.
End	Gives the left pane of the split-screen all of the area (right pane is hidden) if the divider has the focus.
Click + Mouse Drag	Moves the divider left or right.

Table D.2: Tree view control keyboard and mouse shortcuts

Operation	Description
Mouse Single-click	Deselects the existing selection and selects the node the mouse pointer is over.
Mouse Double-click	Toggles the expand and collapse state of an expandable node (a node with sublevels). Does nothing on a leaf node (a node with no sublevels).
Up Arrow	Deselects the existing selection and selects the next node above the current focus point.
Down Arrow	Deselects the existing selection and selects the next node below the current focus point.
Spacebar	Alternately selects and deselects the node that currently has the focus.
Enter	Alternately collapses and expands the node that has focus. Only applies to nodes that have sublevels. Does nothing if a node has no sublevels.
Home	Deselects the existing selection and selects the root node.
End	Deselects the existing selection and selects the last node visible in the tree.

Table D.3: Unit list keyboard and mouse operations

Operation	Description
Enter or **Return**	Starts the default action for the selected unit.
Up Arrow	Deselects current selection and moves selection up one row.
Down Arrow	Deselects current selection and moves selection down one row.
Page Up	Deselects current selection and scrolls up one page, then selects the first item on the page.
Page Down	Deselects current selection and scrolls down one page, then selects the last item on the page.
Delete	Performs the Delete function. Works the same as the **Edit** > **Delete** menu function.
Ctrl + **Home**	Moves the focus and the selection to the first row in the table.
Ctrl + **End**	Moves the focus and the selection to the last row in the table.
Shift + **Up Arrow**	Extends selection up one row.
Shift + **Down Arrow**	Extends selection down one row.
Shift + **Page Up**	Extends selection up one page.
Shift + **Page Down**	Extends selection down one page.
Shift + **Mouse Click**	Deselects any existing selection and selects the range of rows between the current focus point and the row the mouse pointer is over when the mouse is clicked.
Ctrl + **Mouse Click**	Toggles the selection state of the row the mouse pointer is over without affecting the selection state of any other row.
Mouse Double-click	Starts the default action for the selected unit.

Appendix E: Sun Advanced Key Emulation

Certain keys on a standard Type 5 (US) Sun keyboard may be emulated by key press sequences on a PS/2 keyboard. To enable Advanced Sun Key Emulation mode and use they keys, press and hold Ctrl+Shift+Alt and then press the Scroll Lock key. The *Scroll Lock* LED blinks. Use the indicated key in the following table as you would use the advanced keys on a Sun keyboard.

Table E.1: Sun Key Emulation

Sun Key (US)	PS/2 Key Combination
Compose	Application (*)
Compose	keypad*
Power	F11
Open	F7
Help	Num Lock
Props	F3
Front	F5
Stop	F1
Again	F2
Undo	F4
Cut	F10
Copy	F6
Paste	F8
Find	F9
Mute	keypad/
Vol +	keypad +
Vol -	keypad -
Command (left) (**)	F12
Command (left) (**)	Win (GUI) left (*)
Command (right) (**)	Win (GUI) right (*)
(*) Windows 95 104-key keyboard (**) The Command key is the Sun Meta (diamond key)	

For example: For **Stop + A**, press and hold **Ctrl+Shift+Alt** and press **Scroll Lock**, then **F1 + A**.

These key combinations will work with the USB SAM adaptor (if your Sun system comes with a USB port) as well as the Sun SAM adaptor. With the exception of **F12**, these key combinations are not recognized by Microsoft Windows. Using **F12** performs a Windows key press.

Appendix F: Serial Console Viewer Terminal Emulation

The Serial Console Viewer supports several terminal emulation modes. This chapter lists the supported terminal emulation control characters and byte sequences for the modes.

Encode refers to how the client application processes typed keys. Decode refers to how the client application processes data coming from the server.

VT terminal emulation

In the VT terminal emulation modes, when a key on the keypad is entered, it is treated as its label. For example, if you press the **7** on the keypad, it is encoded as a 7. Pressing the key containing a period causes a period to be encoded.

VT100+ terminal emulation

The VT100+ emulation mode provides compatibility with the Microsoft headless server EMS serial port interface. The Serial Console Viewer VT100+ terminal emulation works identically to VT100, with the exception of support for the function keys listed in the following table.

Table F.1: VT100+ Function Key Support

Function	Sequence	Function	Sequence
Home	<Esc> h	F4 **	<Esc> 4
End	<Esc> k	F5	<Esc> 5
Insert	<Esc> +	F6	<Esc> 6
Delete *	<Esc> -	F7	<Esc> 7
Page Up	<Esc> ?	F8	<Esc> 8
Page Down	<Esc> /	F9	<Esc> 9
F1 **	<Esc> 1	F10	<Esc> Ø
F2 **	<Esc> 2	F11	<Esc> !
F3 **	<Esc> 3	F12	<Esc> @

* ASCII, VT100 and VT102 modes send hex 7F when the **Delete** key is pressed.
* VT100 and VT102 modes map the **F1** through **4** keys to the **PF1** through **F4** keys.

VT102 terminal emulation

VT102 terminal emulation works identically to VT100 with additional support for decoding receive codes as described in the following table.

Table F.2: VT102 Receive Codes

VT102 Receive Code	Action
Delete Character (DHC)	Deletes n characters starting with the character at the current cursor position, and moves all remaining characters left npositions. n spaces are inserted at the right margin.
Insert Line (IL)	Inserts n lines at the line where the cursor is currently positioned. Lines displayed below the cursor position move down. Lines moved past the bottom margin are lost.
Delete Line (DL)	Deletes n lines starting with the line where the cursor is currently positioned. As lines are deleted, lines below the cursor position move up.

VT100 terminal emulation

The following table lists the VT100 special key and **Control** key combinations and indicates Black Box encoding/decoding support, where Yes indicates supported and No indicates not supported.

Table F.3: VT100 Special Key and Control Keys

Keys	Hex Code	Function Mnemonic	Encode/Decode
Return	ØD	CR	Yes/Yes
Linefeed	OA	LF	Yes/Yes
Backspace	Ø8	BS	Yes/Yes
Tab	Ø9	HT	Yes/Yes
Spacebar	2Ø	(SP)	Yes/Yes
Esc	1B	ESC	Yes/No
Ctrl+spacebar	ØØ	NUL	Yes/No
Ctrl+A	Ø1	SOH	Yes/No
Ctrl+B	Ø2	STX	Yes/No
Ctrl+C	Ø3	ETX	Yes/No

Table F.3: VT100 Special Key and Control Keys

Keys	Hex Code	Function Mnemonic	Encode/Decode
Ctrl+D	Ø4	EOT	Yes/No
Ctrl+E	Ø5	ENQ	Yes/No
Ctrl+F	Ø6	ACK	Yes/No
Ctrl+G	Ø7	BELL	Yes/Yes
Ctrl+H	Ø8	BS	Yes/Yes
Ctrl+I	Ø9	HT	Yes/Yes
Ctrl+J	ØA	LF	Yes/Yes
Ctrl+K	ØB	VT	Yes/No
Ctrl+L	ØC	FF	Yes/No
Ctrl+M	ØD	CR	Yes/No
Ctrl+N	ØE	SO	Yes/No
Ctrl+O	ØF	SI	Yes/No
Ctrl+P	1Ø	DLE	Yes/No
Ctrl+Q	11	DC1 or XON	Yes/No
Ctrl+R	12	DC2	Yes/No
Ctrl+S	13	DC3 or XOFF	Yes/No
Ctrl+T	14	DC4	Yes/No
Ctrl+U	15	NAK	Yes/No
Ctrl+V	16	SYN	Yes/No
Ctrl+W	17	ETB	Yes/No
Ctrl+X	18	CAN	Yes/No
Ctrl+Y	19	EM	Yes/No
Ctrl+Z	1A	SUB	Yes/No
Ctrl+[	1B	ESC	Yes/No
Ctrl+\	1C	FS	Yes/No
Ctrl+]	1D	GS	Yes/No
Ctrl+~	1E	RS	Yes/No

Table F.3: VT100 Special Key and Control Keys

Keys	Hex Code	Function Mnemonic	Encode/Decode
Ctrl+?	1F	US	Yes/No

The following table lists the VT100 ANSI mode and cursor keys for set and reset modes. Encoding and decoding is supported for all the cursor keys listed.

Table F.4: VT100 ANSI Set and Rest Mode Cursor Keys

Cursor Key	Mode Reset	Mode Set	
Up	Esc [A		Esc O A
Down	Esc [B		Esc O B
Right	Esc [C		Esc O C
Left	Esc [D		Esc O D

The following table lists the VT100 **PF1** through **PF4** key definitions. Encoding of each listed key is supported; decoding is not applicable.

Table F.5: VT100 PF1 through PF4 Key definitions

Key	Code Sequence
F1	Esc [O P
F2	Esc [O Q
F3	Esc [O R
F4	Esc [O S

The following table lists the ANSI mode control sequences for VT100 terminal emulation and indicates Black Box encoding/decoding support, where Yes indicates supported and No indicates not supported.

Table F.6: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
Esc # 4	Double Height Line - Bottom Half	No/No
Esc # 6	Double Width Line	No/No
Esc Z	Identify Terminal	No/No
Esc =	Keypad Application Mode	No/No
Esc >	Keypad Numeric Mode	No/No
Esc [Ps q	Load LEDs	No/No
Esc 8	Restore Cursor	No/Yes
Esc [<sol>; <par>; <nbits>; <xspeed>; <rspeed>; <clkmul>; <flags>x	Report Terminal Parameters	No/No
Esc [<sol> x	Request Terminal Parameters	No/No
Esc 7	Save Cursor	No/Yes
Esc [Pn; Pn r	Set Top and Bottom Margins	No/No
Esc # 5	Single Width Line	No/No

Table F.6: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
Esc [2; Ps y	Invoke Confidence Test	No/No
Esc [Ps n	Device Status Report	No/Yes
Esc [Ps J	Erase in Display	No/Yes
Esc [Ps K	Erase in Line	No/Yes
Esc H	Horizontal Tabulation Set	No/No
Esc [Pn; Pn f	Horizontal and Vertical Position	No/Yes
Esc D	Index	No/Yes
Esc E	Next Line	No/Yes
Esc M	Reverse Index	No/Yes
Esc c	Reset to Initial State	No/No
Esc [Ps; Ps;..;Ps 1	Reset Mode	No/No
Esc (A	Select Character Set GØ U.K.	No/No
Esc) A	Select Character Set G1 U.K.	No/No
Esc (B	Select Character Set GØ ASCII	No/No
Esc) B	Select Character Set G1 ASCII	No/No

Table F.6: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
Esc (Ø	Select Character Set GØ Spec. Graphics	No/No
Control Sequence	Definition	Encode/Decode
Esc) Ø	Select Character Set G1	
	Spec. Graphics	No/No
Esc (1	Select Character Set GØ	
	Alt. Character ROM Standard	
	Character Set	No/No
Esc) 1	Select Character Set G1 Alt. Character ROM Standard Character Set	No/No
Esc (2	Select Character Set GØ Alt. Character ROM Special Graphics	No/No
Esc) 2	Select Character Set G1 Alt. Character ROM Special Graphics	No/No
Esc [Ps;..; Ps m	Select Graphic Rendition	No/No
Esc Ps;..;Ps h	Set Mode	No/No
Esc [Ps g	Tabulation Clear	No/No

Table F.6: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
Esc [Ps;Ps;..; Ps m	Character Attributes Ø or none - All attributes Off 1 - Bold On, 4 - Underscore On 5 - Blink On, 7 - Reverse Video On	No/Reverse and Bold supported; Blink and Under-score appear as italic
Esc [K or Esc [Ø K	Erase from cursor to end of line	No/Yes
Esc [1 K	Erase from beginning of line to cursor	No/No
Esc [2 K	Erase entire line containing cursor	No/No
Esc [J or Esc [Ø J	Erase from cursor to end of screen	No/Yes
Esc [1 J	Erase from beginning of screen to cursor	No/No
Esc [2 J	Erase entire screen	No/No
Esc [Ps;Ps;..Ps q	Programmable LEDs	No/No
Esc [Pt; Pb r	Scrolling Region	No/No
Esc H	Set tab at current column	No/No
Esc [g or Esc [Ø g	Clear tab at current column	No/No
Esc [3 g	Clear all tabs	No/No

Table F.6: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
Control Sequence	Definition	Encode/Decode
Esc [2 Ø h	Modes to Set - New Line Only supports linefeed/ new line column mode wraparound	No/Yes ->
Esc [2 Ø l	Modes to Reset - Linefeed Only supports linefeed/ new line column mode wraparound	No/Yes ->
Esc [? 1 h	Modes to Set - Cursor Key Mode Appl.	No/No
Esc [? 1 l	Modes to Reset - Cursor Key Mode Cursor	No/No
Esc [? 2 l	Modes to Reset VT52	No/No
Esc [? 3 h	Modes to Set - 132 columns	No/No
Esc [? 3 l	Modes to Reset - 80 columns	No/No
Esc [? 4 h	Modes to Set - Smooth Scroll	No/No
Esc [? 4 l	Modes to Reset - Jump Scroll	No/No
Esc [? 5 h	Modes to Set - Reverse	

Table F.6: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
	Screen Mode	No/No
Esc [? 5 l	Modes to Reset - Normal	
	Screen Mode	No/No
Esc [? 6 h	Modes to Set - Relative	
	Origin Mode	No/No
Esc [? 6 l	Modes to Reset - Absolute	
	Origin Mode	No/No
Esc [? 7 h	Modes to Set - Wraparound On	No/No
Esc [? 7 l	Modes to Reset - Wraparound Off	No/No
Esc [? 8 h	Modes to Set - Auto Repeat On	No/No
Esc [? 8 l	Modes to Reset - Auto Repeat Off	No/No
Esc [? 9 h	Modes to Set - Interlace On	No/No
Esc [? 9 l	Modes to Reset - Interlace Off	No/No
Esc [6 n	Report Cursor Position - Invoked by	No/No

Table F.6: VT100 ANSI Mode Control Sequences

Control Sequence	Definition	Encode/Decode
Esc [Pn; Pn R	Cursor Position Report	No/No
Esc [Pn D	Cursor Backward	No/Yes
Esc [Pn B	Cursor Down	No/Yes
Esc [Pn C	Cursor Forward	No/Yes
Esc [Pn; Pn H	Cursor Position	No/Yes
Esc [Pn A	Cursor Up	No/Yes
Esc [Pn c	Device Attributes	No/No
Esc # 8	Screen Alignment Display	No/Yes
Esc # 3	Double Height Line - Top Half	No/No
Esc [P1; Pc R	Report Cursor Position - Response is	No/No
Esc [5 n	Status Report - Invoked by	No/No
Esc [Ø n	Status Report - Response is terminal OK	No/No
Control Sequence	Definition	Encode/Decode
Esc [3 n	Status Rpt - Response is terminal not OK	No/No
Esc [x or Esc [Ø c	What are you? Invoked by	No/No
Esc [? 1; Ps c	What are you? Response is	No/No
Esc c	Reset	No/No
Esc # 8	Fill screen with Es	No/Yes
Esc [2; Ps y	Invoke Test(s)	No/No

VT220 terminal emulation

The following table lists the keystroke mapping (encoding) for VT220 emulation.

Table F.7: VT220 Encoding

VT220 Keyboard	PC Keyboard	VT200 KB Byte Sequence
Delete	Delete	Øx7F

Table F.7: VT220 Encoding

VT220 Keyboard	PC Keyboard	VT200 KB Byte Sequence
Left Arrow	Left Arrow	ESC [D
Right Arrow	Right Arrow	ESC [C
Up Arrow	Up Arrow	ESC [A
Down Arrow	Down Arrow	ESC [B
Keypad /	Keypad /	/
Keypad *	Keypad *	*
Keypad -	Keypad -	-
Keypad +	Keypad +	+
Keypad .	Keypad .	.
Keypad Ø..9	Keypad Ø..9	Ø..9
F1	F1	Esc O P
F2	F2	Esc O Q
F3	F3	Esc O R
F4	F4	Esc O S
F6	F6	Esc [1 7 ~
F7	F7	Esc [1 8 ~
F8	F8	Esc [1 9 ~
F9	F9	Esc [2 Ø ~
F10	F10	Esc [2 1 ~
F11	F11	Esc [2 3 ~
F12	F12	Esc [2 4 ~
F13	Ctrl - F5	Esc [2 5 ~
F14	Ctrl - F6	Esc [2 6 ~
F15	Ctrl - F7	Esc [2 8 ~
F16	Ctrl - F8	Esc [2 9 ~
F17	Ctrl - F9	Esc [3 1 ~
F18	Ctrl - F10	Esc [3 2 ~
F19	Ctrl - F11	Esc [3 3 ~

Table F.7: VT220 Encoding

VT220 Keyboard	PC Keyboard	VT200 KB Byte Sequence
F20	Ctrl - F12	Esc [3 4 ~

The following table lists the VT220 terminal emulation decoding.

Table F.8: VT220 Decoding

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Index	Esc D
New Line	Esc E
Reverse Index	Esc M
Escape O	Esc O
Save cursor and attributes	Esc 7
Restore cursor and attributes	Esc 8
Up Arrow	Esc [A
Down Arrow	Esc [B
Right Arrow	Esc [C
Left Arrow	Esc [D
Set cursor to home position	Esc [H
Set cursor to home position	Esc [f
Character attributes	Esc [m
Erase from cursor to end of line	Esc [K
Erase from cursor to end of screen	Esc [J
Programmable LEDs	Esc [q
What are You?	Esc [c
Set Mode	Esc [?
Delete 1 Character	Esc [P
Insert 1 Line	Esc [L
Delete 1 Line	Esc [M
Up Arrow	Esc O A

Table F.8: VT220 Decoding

VT220 Keyboard Function	VT220 Keyboard Byte Sequence
Down Arrow	Esc O B
Right Arrow	Esc O C
Left Arrow	Esc O D
Fill Screen with Es	Esc # 8
Up Arrow amount specified by Pn	Esc [Pn A
Down Arrow amount specified by Pn	Esc [Pn B
Right Arrow amount specified by Pn	Esc [Pn C
Left Arrow amount specified by Pn	Esc [Pn D
Erase parts of current line	Esc [Pn K
Erase parts of current screen	Esc [Pn J
Direct Cursor Addressing	Esc [Pn H
Direct Cursor Addressing	Esc [Pn f
Programmable LEDs	Esc [Pn q
Scrolling Region	Esc [Pn r
Clear tabs	Esc [Pn g
Device status report	Esc [Pn n
What are you?	Esc [Pn c
Set Mode	Esc [Pn h
Delete Pn Characters	Esc [Pn P
Insert Pn Lines	Esc [Pn L
Delete Pn Lines	Esc [Pn M
Insert Character	Esc [Pn @
Erase Pn Characters	Esc [Pn X

VT52 terminal emulation

The following table lists the keystroke mapping (encoding) for VT52 terminal emulation.

Table F.9: VT52 Encoding

VT52 Keyboard	PC Character Sequence	VT52 Keyboard Byte Sequence
Delete	Delete	Øx7F
Up Arrow	Up Arrow	Esc A
Down Arrow	Down Arrow	Esc B
Right Arrow	Right Arrow	Esc C
Left Arrow	Left Arrow	Esc D
Shift-F1	PF1	Esc P
Shift-F2	PF2	Esc Q
Shift-F3	PF3	Esc R
Shift-F4	PF4	Esc S

The following table lists the decoding for VT52 terminal emulation.

Table F.10: VT52 Decoding

VT52 Keyboard Function	VT52 Keyboard Byte Sequence
Cursor Up	Esc A
Cursor Down	Esc B
Cursor Right	Esc C
Cursor Left	Esc D
Cursor Home	Esc H
Reverse Linefeed	Esc I
Erase to end of screen	Esc J
Erase to end of line	Esc K

VT320 terminal emulation

The following table lists keystroke mapping (encoding) for VT320 terminal emulation.

Table F.11: VT320 Encoding

VT320 Keyboard	PC Character Sequence	VT320 Keyboard Byte Sequence
Escape key	Esc	Øx1B
F1	F1	Esc O P
F2	F2	Esc O Q
F3	F3	Esc O R
F4	F4	Esc O S
F5	F5	Esc O T
F6	F6	Esc [1 7 ~
F7	F7	Esc [1 8 ~
F8	F8	Esc [1 9 ~
F9	F9	Esc [2 Ø ~
F10	F10	Esc [2 1 ~
F11	F11	Esc [2 3 ~
F12	F12	Esc [2 4 ~
F13	Ctrl - F5	Esc [2 5 ~
F14	Ctrl - F6	Esc [2 6 ~
F15	Ctrl - F7	Esc [2 8 ~
F16	Ctrl - F8	Esc [2 9 ~
F17	Ctrl - F9	Esc [3 1 ~
F18	Ctrl - F10	Esc [3 2 ~
F19	Ctrl - F11	Esc [3 3 ~
F20	Ctrl - F12	Esc [3 4 ~
Insert	Insert	Esc [1 ~
Home	Home	Esc [2 ~
Delete	Delete	Øx7F

Table F.11: VT320 Encoding

VT320 Keyboard	PC Character Sequence	VT320 Keyboard Byte Sequence
End	End	Esc [5 ~
Up Arrow	Up Arrow	Esc [A
Down Arrow	Down Arrow	Esc [B
Left Arrow	Left Arrow	Esc [D
Right Arrow	Right Arrow	Esc [C

The following table lists the decoding for VT320 terminal emulation.

Table F.12: VT320 Decoding

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Index	Esc D
New Line	Esc E
Reverse Index	Esc M
Escape O	Esc O
Save cursor and attributes	Esc 7
Restore cursor and attributes	Esc 8
Up Arrow	Esc [A
Down Arrow	Esc [B
Right Arrow	Esc [C
Left Arrow	Esc [D
Set cursor to home position	Esc [H
Set cursor to home position	Esc [f
Character Attributes	Esc [m
Erase from cursor to end of line	Esc [K
Erase from cursor to end of screen	Esc [J
Programmable LEDs	Esc [q
What are You?	Esc [c
Set Mode	Esc [?

Table F.12: VT320 Decoding

VT320 Keyboard Function	VT320 Keyboard Byte Sequence
Delete 1 Character	Esc [P
Insert 1 Line	Esc [L
Delete 1 Line	Esc [M
Up Arrow	Esc O A
Down Arrow	Esc O B
Right Arrow	Esc O C
Left Arrow	Esc O D
Fill Screen with Es	Esc # 8
Up Arrow amount specified by Pn	Esc [Pn A
Down Arrow amount specified by Pn	Esc [Pn B
Right Arrow amount specified by Pn	Esc [Pn C
Left Arrow amount specified by Pn	Esc [Pn D
Erase parts of current line	Esc [Pn K
Erase parts of current screen	Esc [Pn J
Direct Cursor Addressing	Esc [Pn H
Direct Cursor Addressing	Esc [Pn f
Programmable LEDs	Esc [Pn q
Scrolling Region	Esc [Pn r
Clear tabs	Esc [Pn g
Device status report	Esc [Pn n
What are you?	Esc [Pn c
Set Mode	Esc [Pn h
Delete Pn Characters	Esc [Pn P
Insert Pn Lines	Esc [Pn L
Delete Pn Lines	Esc [Pn M
Insert Character	Esc [Pn @
Erase Pn Characters	Esc [Pn X

Appendix G: Ports used by the software

Table G.1 lists the port numbers that the software uses to communicate with certain appliances. This information can be used to configure firewalls to let ServSelect IP Software operate in the networks.

Table G.1: Ports Used by ServSelect IP Software

Port Number	Appliance	Type	Purpose
3211	KV2116, KV4116, or ServSelect III VM	TCP	Proprietary management protocol
3211	KV2116, KV4116, or ServSelect III VM	UDP	Proprietary install and discovery protocol
2068	KV2116, KV4116, or ServSelect III VM	TCP	Encrypted keyboard and mouse data
2068	KV4116 or KV2116	TCP	Digitized video data
2068	KV4116 or KV2116	TCP	Virtual media
8192	ServSelect III VM	TCP	Digitized video data

Appendix H: Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Black Box products, you will find a wide variety of sources available from Black Box to assist you. This appendix contains information about where to go for additional information about Black Box and Black Box products and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the Hardware Maintenance Manual and Troubleshooting Guide or Problem Determination and Service Guide on the Black Box Documentation CD that comes with your system.
- Go to the Black Box support Web site at http://www.blackbox.com to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by following the troubleshooting procedures that Black Box provides in the online help or in the documentation that is provided with your Black Box product.

Using the documentation

Information about your Black Box software is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. Black Box maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.blackbox.com and follow the instructions.

Appendix I: Notices

Trademarks

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adaptec and HostRAID are trademarks of Adaptec, Inc., in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat, the Red Hat “Shadow Man” logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

INDEX

A

Access levels
- KV2116 and KV4116 appliances **71**

AMP
- about **55**
- accessing **18, 55**
- changing global network values **56**
- changing global session values **60**
- exiting **56**
- managing user sessions **75**
- rebooting the appliances **89**
- resynchronizing the device list **82**
- upgrading firmware **86**
- user accounts **71**
- viewing SAM cable information **76**
- viewing device connection information **82**
- See also *Databases*, *Firmware*, *SNMP*, and *User accounts*

Appliances
- accessing **18**
- adding **15**
- assigning **27**
- deleting **28**
- renaming **29**

Assignment **27**

Authentication **62**

B

Browser
- configuring application to launch **25**
- configuring generic appliance URL **22**
- requirements **8**

C

SAM cables
- adding **16, 84**
- upgrading firmware individually **89**
- upgrading firmware simultaneously **88**
- viewing information **76, 82**

Components of ServSelect IP Software **2**

Connection
- multiple connections **4**

Credentials
- setting for device from Thumbnail Viewer **41**

credentials **18, 19**
- cached **18, 19**

Custom label fields in Explorer **24**

D

Databases
- exporting the local ServSelect IP Software database **30**
- loading the local ServSelect IP Software database **30**
- restoring a KV2116 and KV4116 appliances configuration database **91**
- restoring KV2116 and KV4116 appliances user database **92**
- saving a KV2116 and KV4116 appliances configuration database **90**
- saving a KV2116 and KV4116 appliances user database **92**
- saving the local ServSelect IP Software database **30**

ServSelect IP Software local database **29**
DCHP (KV2116 and KV4116 appliances) **56**
Department
deleting **28**
renaming **29**
specifying in properties **21**
Devices
accessing **19**
assigning **27**
auto searching in Unit list **20**
changing network properties **22**
deleting **28**
name displays **4**
naming **4**
renaming **29**
resynchronizing the list (KV2116 and KV4116 appliances) **82**
searching in local database **20**
viewing connection information (KV2116 and KV4116 appliances) **82**
viewing connection properties **23**
DirectDraw **25**

E

Encryption
keyboard/mouse for KV2116 and KV4116 appliances **60**
specifying for virtual media sessions **52**
when saving/restoring configuration databases (KV2116 and KV4116 appliances) **90**
Explorer
accessing appliances **18**
accessing devices **19**
adding appliances **15**
changing custom field labels **24**
changing properties **21**
changing the view on startup **25**
keyboard and mouse shortcuts **96**
window features **13**

F

Features and benefits **1**
Firmware
displaying KV2116 and KV4116 appliances and SAM cable version numbers **86**
upgrading SAM cables individually **89**
upgrading SAM cables simultaneously **88**
upgrading KV2116 and KV4116 appliances **87**
Folders
assigning a unit to **27, 28**
creating **26**
deleting **28**
renaming **29**
Full screen mode (Video Viewer) **43**

G

Gateway
changing for KV2116 and KV4116 appliances **56**
KV2116 and KV4116 appliances
accessing **18**
adding **15**
quick setup **11**
See also *AMP*
KV2116 and KV4116 database **90, 91**
Glossary **3**

H

Hardware requirements **7**

I

Installation **8**

IP address
changing for KV2116 and KV4116 appliances **56**

K

Keyboard
configuring encryption level for KV2116 and KV4116 appliances **60**
shortcuts in Explorer **96**

L

LAN speed (KV2116 and KV4116 appliances) **56**
LDAP
Active Directory **63, 70**
authentication **63**
query modes **68**
query parameters **66**
search parameters **65**
server parameters **64**
Licensed options **86**
Location
assigning a unit to **27, 28**
specifying in properties **21**
Lock-out. See *Security lock-out*

M

Macros (Video Viewer)
displaying a macro group **49**
sending **49**
using **48**
Microsoft Windows
installing on **8**
launching on **10**
supported operating systems **7**
uninstalling on **9**
Mouse (Video Viewer)
adjusting options **45**
aligning cursor **42**
changing cursor settting **45**
realigning **46**
setting encryption level **60**
setting scaling **46**
Mouse shortcuts in Explorer **96**
Multiple connections **4**

N

Network settings
KV2116 and KV4116 appliances **56**

O

Operating systems **7**

P

Ports used by VC software **98**
Preemption
considerations in virtual media sessions **50**
Preemption of local user on Video Viewer **36**
Properties
about changing in Explorer **21**
changing general properties in Explorer **21**
changing information properties in Explorer **22**
changing network properties in Explorer **22**

Q

Quick setup
KV2116 and KV4116 appliances **11**
ServSelect IP Software **10**

R

Reboot
KV2116 and KV4116 appliances **89**
Red Hat Linux

installation on **8**
launching on **10**
supported operating systems **7**
uninstalling on **9**
Requirements
virtual media **50**
Resynchronization **82**

S

Scaling (Video Viewer)
enabling automatic or manual **43**
setting for mouse **46**
Scan mode (Video Viewer)
accessing **39**
changing the thumbnail size **40**
disabling a device thumbnail in the scan sequence **40**
enabling a device thumbnail in the scan sequence **40**
launching a session to a device **40**
setting device credentials **41**
Security lock-out
KV2116 and KV4116 appliances **74**
Sessions
closing a virtual media session **54**
Site
assigning a unit to **27, 28**
deleting **28**
renaming **29**
specifying in properties **21**
SNMP (KV2116 and KV4116 appliances)
configuring general settings **78**
enabling/disabling traps **80**
using **78**
Subnet mask
changing for KV2116 and KV4116 appliances **56**

T

Time-out values
Video Viewer sessions **60**
Type
deleting **28**
renaming **29**
specifying in properties for devices **21**

U

User accounts (KV2116 and KV4116 appliances)
about locking/unlocking **74**
access levels **71**
adding **72**
deleting **73**
enabling/disabling security lock-out **74**
modifying **72**
unlocking **74**
User sessions
KV2116 and KV4116 appliances **75**

V

VM SAM USB2-VGA cables
required for virtual media **50**
ServSelect IP Software
about **1**
installing **8**
ports used **98**
quick setup **10**
system components **2**
Video Viewer
about **31**
accessing **31**
adjusting the view **36, 43**

changing session time-out value **60**
closing a session **32**
enabling automatic/manual scaling **43**
enabling/disabling DirectDraw **25**
enabling/disabling full screen mode **43**
macros **48**
preempting local user **36**
refreshing the screen **42**
See also *Macros*, *Mouse* and *Scan mode*
window features **32**
Virtual media
closing a session **54**
displaying drive details **53**
encryption level **52**
locking to KVM session **51**
mapped drive access mode **52**
mapping drives **52**
requirements **50**
reserved sessions **50**
resetting USB devices on the target device **53**
session settings **51**
sharing and preemption considerations **50**
unmapping drives **53**
window **50**

W

Window features
Explorer **13**
Video Viewer **32**